VES-1616/24FA-5x Series
VDSL Switch

Support Notes

Version1.0
Apr. 2008

ZyXEL
Unleash Networking Power

Switch Management and Maintenance ----3
Firmware Upgrade ----3
Using the Web Configurator ----3
Using the Console Port: ----3
Using FTP: ----4
Restore a Configuration File ----4
Using the Web Configurator: ----4
Using the Console Port: ----5
Using FTP: ----5
Backing Up a Configuration File ----6
Using the Web Configurator: ----6
Using the Console Port: ----6
Using FTP: ----7
Load Factory Defaults ----7
Using the Web Configurator: ----7
Using the Console Port: ----8
General Networking ----8
DHCP Relay Option 82 Application ----8
Setting up a DHCP Relay Option 82 Environment ----9
Separating a physical network into multiple virtual networks ----24
What is Virtual LAN? ----24
VLAN Overview ----24
Port-based VLAN ----25
Port-based VLAN across multiple switches ----27
How to configure Port-Based VLAN ----28
What is IEEE 802.1Q Tag-based VLAN? ----33
How 802.1Q VLAN works ----34
Connecting Two Switches using VLAN ----37
Setting up VLAN Trunking ----40
VLAN Stacking Overview ----44
Configuring Switch A, E, F and H Using the Web Configurator ----46
Configuring Switch B Using the Web Configurator ----46
Configuring Switch C Using the Web Configurator ----50
Configuring Switch D Using the Web Configurator ----52
Configuring Switch G Using the Web Configurator ----55
Network Scenario ----59
Configuring Switches A, E, F and H Using the CLI ----59
Configuring Switch B Using the CLI ----60
Configuring Switch C via CLI ----61
Configuring Switch D Using the CLI ----62
IP Multicasting ----64
Configuring IGMP snooping in your switch ----64
Configuration of IGMP snooping by web ----65
Configuration of IGMP and IGMP snooping by CLI ----66
Overview of MVR ----67
MVR Mode ----68

All contents copyright 2008 ZyXEL Communications Corporation.

Operation Mode ---- 69
Scenario of MVR ---- 69
Triple play Application ---- 77
Configure VES-1616FA-54 ---- 77
Configure P-870H-51 ---- 82
Ringing a network by building redundant links and connections between Switch ---- 91
What is Spanning Tree Protocol? ---- 91
Spanning Tree Overview ---- 91
How STP Works ---- 92
How STP works ---- 94
Switching security ---- 96
MAC Limit ---- 96
Setting up 802.1x Radius Authentication. ---- 98
Port Authentication: RADIUS Setup ---- 98
RADIUS Server Setup ---- 99
Create User Account ---- 99
Supplicant Setup (Windows XP) ---- 99
802.1x/MD5-challenge setup ---- 100
Classifier & Policy rule setup on your Switch ---- 102
Classifier Configuration ---- 103
Policy Rule Configuration ---- 104
Centralized Management ---- 105
Introduction to SNMPc and NetAtlas ---- 105
SNMPc Overview ---- 106
EMS Overview ---- 107
FAQ ---- 114
What are the default IP parameter settings? ---- 114
What is the default login Name and Password to log into the Web Configurator? ---- 114
How to access my SWITCH through the console port? ---- 114
What is default login password for console, telnet, and FTP login? ---- 114
How to change the password? ---- 114
How to access the Command Line Interface (CLI)? ---- 115
If I have forgotten the password, how to reset the password to the default setting? ---- 115
How to configure the IP address? ---- 115
Is Online Help available on the Web Configurator? ---- 116
How to restart device from the Web Configurator? ---- 116
How to check the current running firmware version? ---- 116
Is the mini GBIC transceiver hot-swappable? ---- 117
What is "Dual-Personality interface" on a VDSL Switch? ---- 117
Can I enable IGMP snooping on the Switch which is acting as an IGMP Router? ---- 117
Can I enable MVR and IGMP snooping at the same time? ---- 117

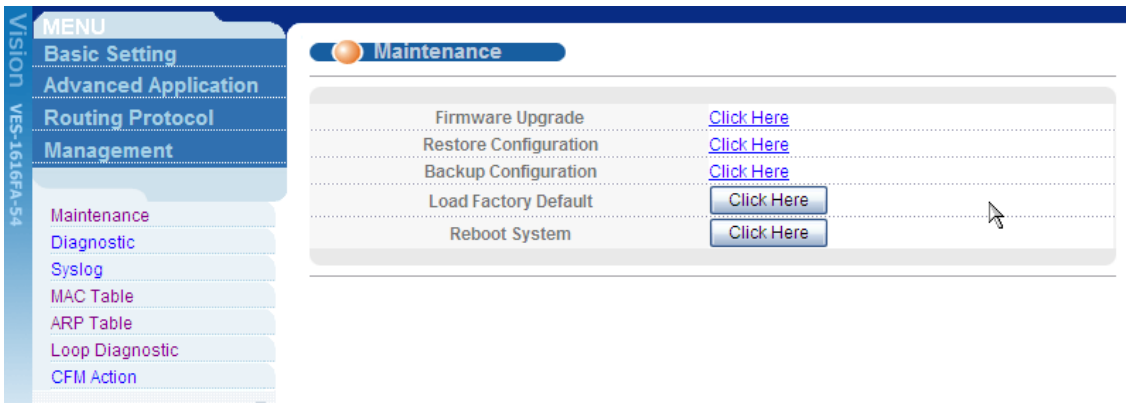
All contents copyright 2008 ZyXEL Communications Corporation.

Switch Management and Maintenance

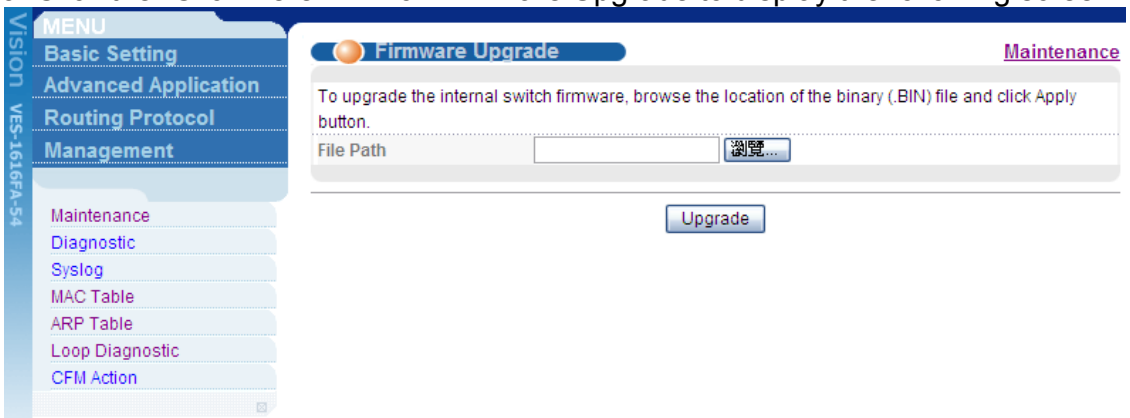
Firmware Upgrade

Using the Web Configurator

1. Download (and unzipped) the correct model firmware to your computer.
2. Click Management > Maintenance in the navigator panel to display the following screen.



3. Click the “Click Here” link for Firmware Upgrade to display the following screen.



4. In the File Path field, click Browse to locate the firmware file.
5. Click Upgrade to start the firmware upgrade process.

Using the Console Port:

All contents copyright 2008 ZyXEL Communications Corporation.

1. Download (and unzipped) the correct model firmware to your computer.
2. Connect to the console port and launch a Terminal Emulation software
3. Restart the switch to enter the debug mode via the terminal.
4. Enter “ATUR”.
5. Use the X-modem protocol to transfer (Send File) the firmware.
6. Enter “ATGO” to restart the switch after the file transfer is complete and the firmware upgrade process is done.

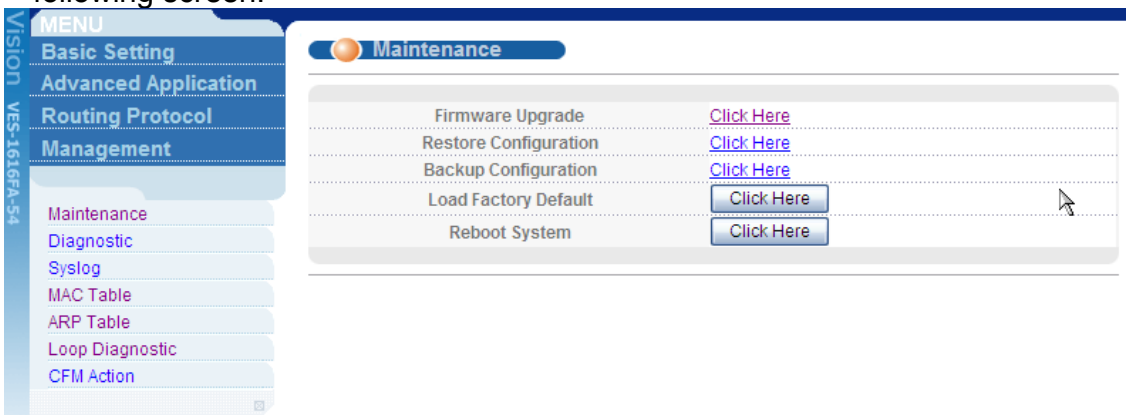
Using FTP:

1. Download (and unzipped) the correct model firmware to your computer.
2. Launch the FTP client on your computer to log into switch. (From the command prompt, type “ftp <Switch IP>”).
3. Press [ENTER] when prompted for a user name.
4. Enter the administrator login password to access the switch and display FTP prompt.
5. Enter “bin” to set the transfer mode to binary.
6. Use “put” to transfer the firmware from the computer to the switch, for example: “put firmware.bin ras-0” transfers the firmware on your computer (firmware.bin) to the switch and renames it to “ras-0”.
7. Use “put” to transfer the firmware from the computer to the switch, for example: “put firmware.bin ras-1” transfers the firmware on your computer (firmware.bin) to the switch and renames it to “ras-1”.
8. Enter “bye” to log out from the switch.

Restore a Configuration File

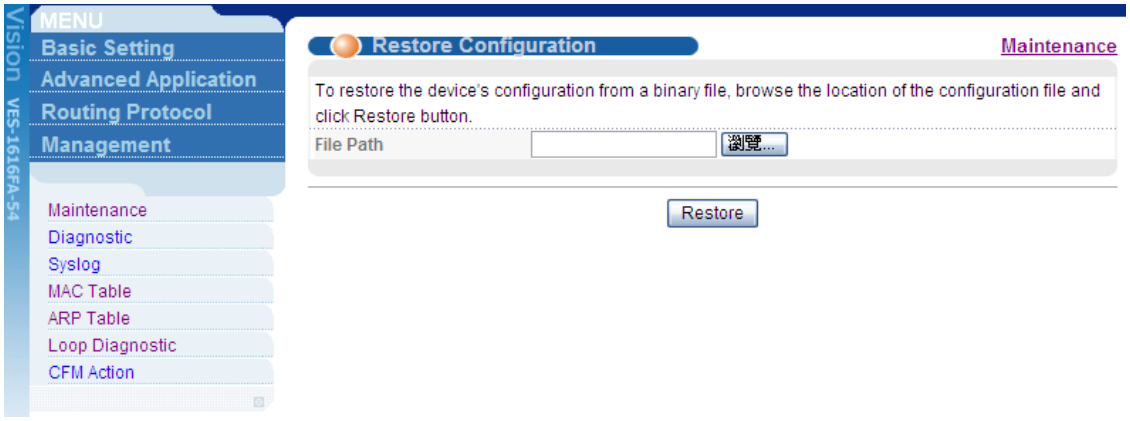
Using the Web Configurator:

1. Click Management > Maintenance in the navigator panel to display the following screen.



All contents copyright 2008 ZyXEL Communications Corporation.

2. Click the “Click Here” link for Restore Configuration to display the following screen.



3. In the File Path field, click Browse to locate the firmware file.
4. Click Restore to start restoring configuration.

Using the Console Port:

1. Connect to the console port and launch a Terminal Emulation software.
2. Restart the switch to enter the debug mode via the terminal.
3. Enter “ATLC”
4. Use X-modem protocol to transfer (Send File) the configuration file (with a .rom file extension).
5. Enter “ATGO” to restart the switch after file transfer and the configuration restore processes are complete.

Using FTP:

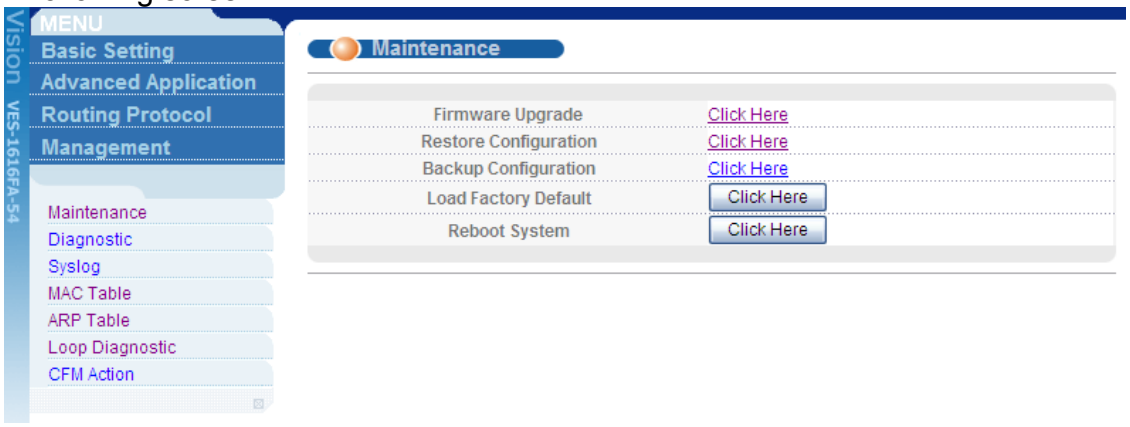
1. Download (and unzipped) the correct model firmware to your computer.
2. Launch the FTP client on your computer to log into the switch. (From the command prompt, type “ftp <Switch IP>”.
3. Press [ENTER] when prompted for a user name
4. Enter the administrator login password to access the switch and display FTP prompt.
5. Enter “bin” to set the transfer mode to binary.
6. Use “put” to transfer the configuration file from the computer to the switch, for example: “put comfig.rom config” transfers the configuration file on your computer (config.rom) to the switch and renames it to “config”.
7. Enter “bye” to log out from the switch.

All contents copyright 2008 ZyXEL Communications Corporation.

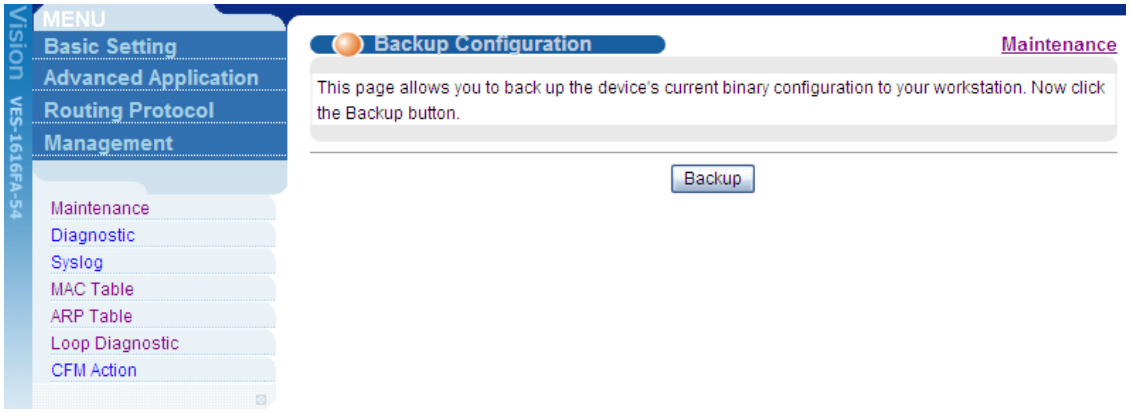
Backing Up a Configuration File

Using the Web Configurator:

1. Click Management > Maintenance in the navigator panel to display the following screen.



2. Click the “Click Here” link for Backup Configuration to display the following screen.



3. Click Backup to display the File Download dialog. Then, click Save to back up the configuration text file to a location you specify on your computer.

Using the Console Port:

1. Connect to the console port and launch a Terminal Emulation software.
2. Restart the switch to enter the debug mode via the terminal.
3. Enter “ATTD”.
4. Use X-modem protocol to transfer (Receive File) the configuration file (with a .rom file extension).

All contents copyright 2008 ZyXEL Communications Corporation.

5. Enter “ATGO” to restart the switch after file transfer and the configuration backup processes are complete. .

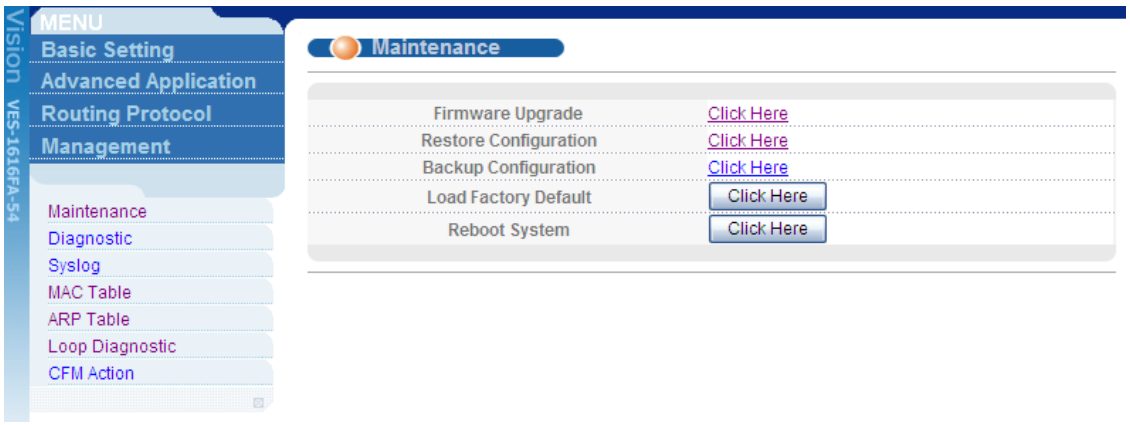
Using FTP:

1. Download (and unzipped) the correct model firmware to your computer.
2. Launch the FTP client on your PC to log into the switch. (From the command prompt, type “ftp <Switch IP>”
3. Press [ENTER] when prompted for a user name
4. Enter the administrator login password to access the switch and display FTP prompt.
5. Enter “bin” to set the transfer mode to binary.
6. Use “get” to transfer the configuration file from the switch to your computer, for example: “get config config.rom” transfers the configuration file on the switch (config) to your computer and renames it “config.rom”.
7. Enter “bye” to log out from the switch.

Load Factory Defaults

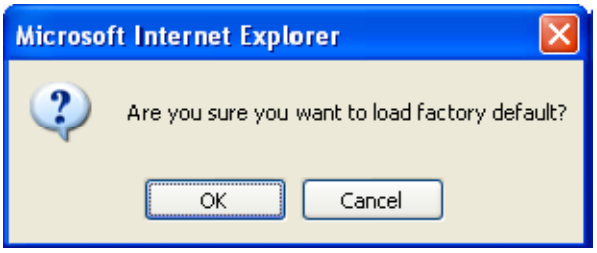
Using the Web Configurator:

1. Click Management > Maintenance in the navigation panel to display the following screen.



2. Click “Click Here” link for Load Factory Default.
3. A dialog box pops up with the “Are you sure you want to load factory defaults?” prompt.

All contents copyright 2008 ZyXEL Communications Corporation.



4. Click OK.
5. Click OK again to start the configuration reset process.
6. Please note that the IP address of the switch is now 192.168.1.1.

Using the Console Port:

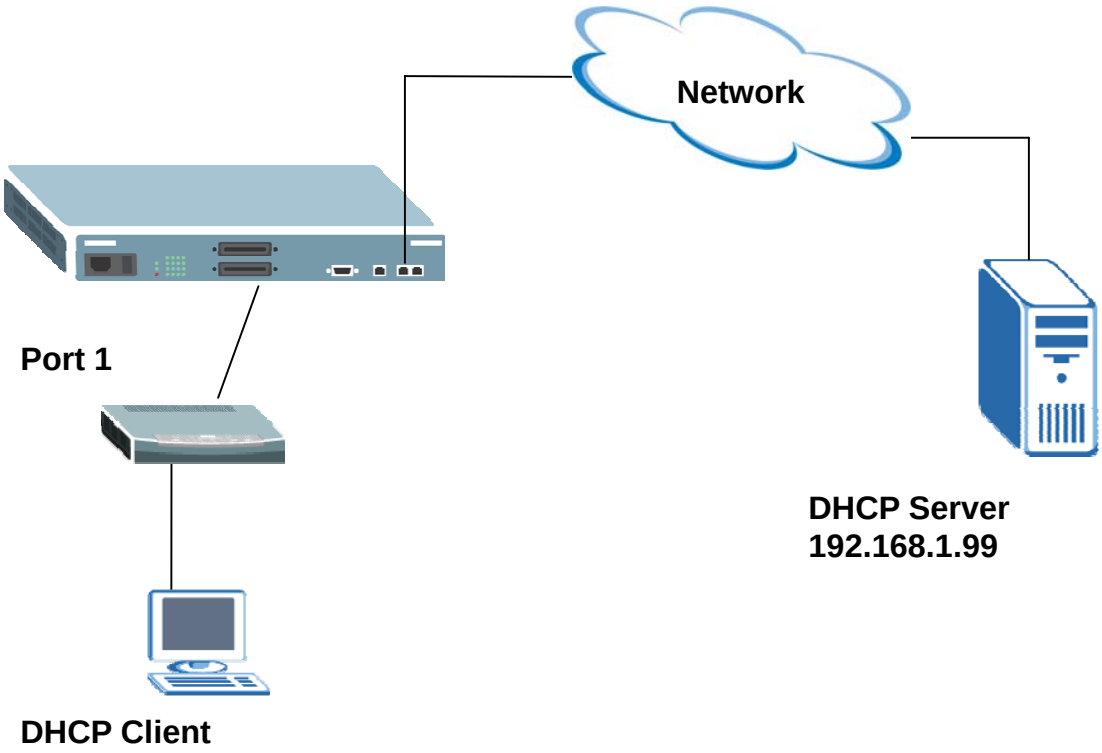
1. Connect to the console port and open the Terminal Emulation Software.
2. Enter the administrator login password to log into the CLI. Enter “erase run” to load the factory default configuration.

General Networking

DHCP Relay Option 82 Application

ISP may want to limit the number of IP address or provide some specific client IP addresses based on the switch ports, VLAN ID and option 82 string.
They can easily achieve this with the DHCP Relay Option 82 feature and a DHCP server that supports Option 82.
The following figure shows a network example.

All contents copyright 2008 ZyXEL Communications Corporation.



Setting up a DHCP Relay Option 82 Environment

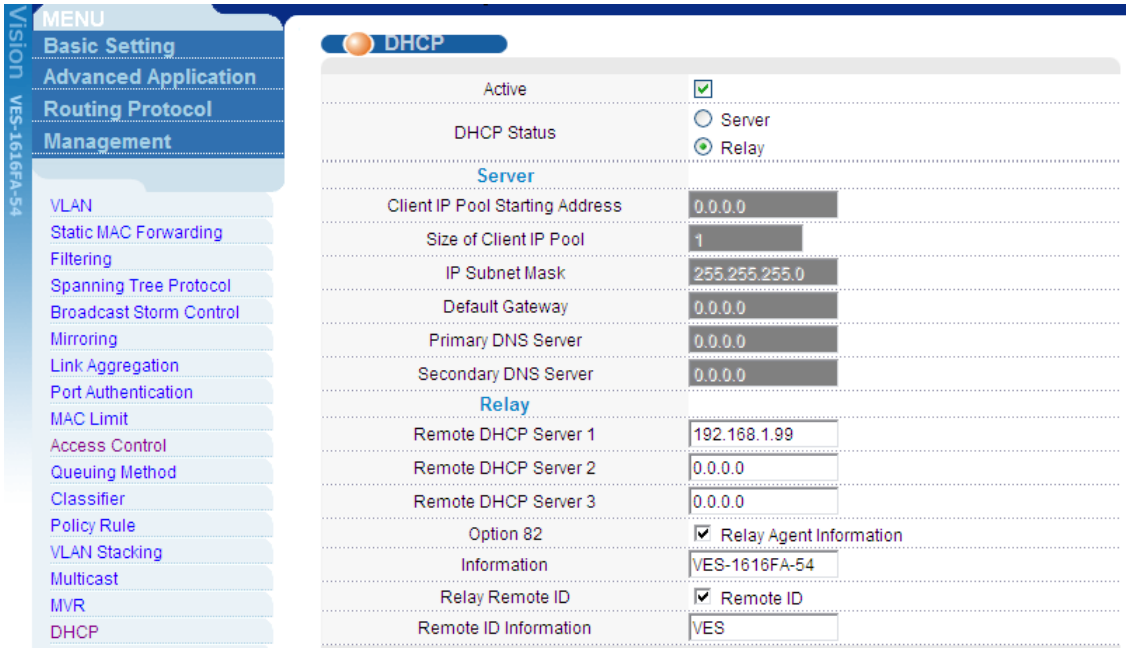
In this example, we will show you how to configure DHCP relay settings to allow a computer to obtain a specific IP address from a DHCP server based on the VDSL port, VLAN ID and the Option82 string.

In this network environment, we will use a VES-1616FA-5x series with a computer connected to a CPE to the first VDSL port. The Option82 string is set to "VES-1616FA-54".
The IP address of the DHCP server (IP Commander at 192.168.1.99) and it is to assign client IP addresses of 192.168.1.201 and 192.168.1.203 for VLAN ID 1 with Option82 string of "VES-1616FA-54".

1. Switch settings

In the web configurator, click **Advanced Application > DHCP** in the navigation panel to display the **DHCP** screen as shown. Enable the DHCP relay feature and the Option 82 function. Click **Information** to set "VES-1616FA-54" as the Option 82 string.

All contents copyright 2008 ZyXEL Communications Corporation.

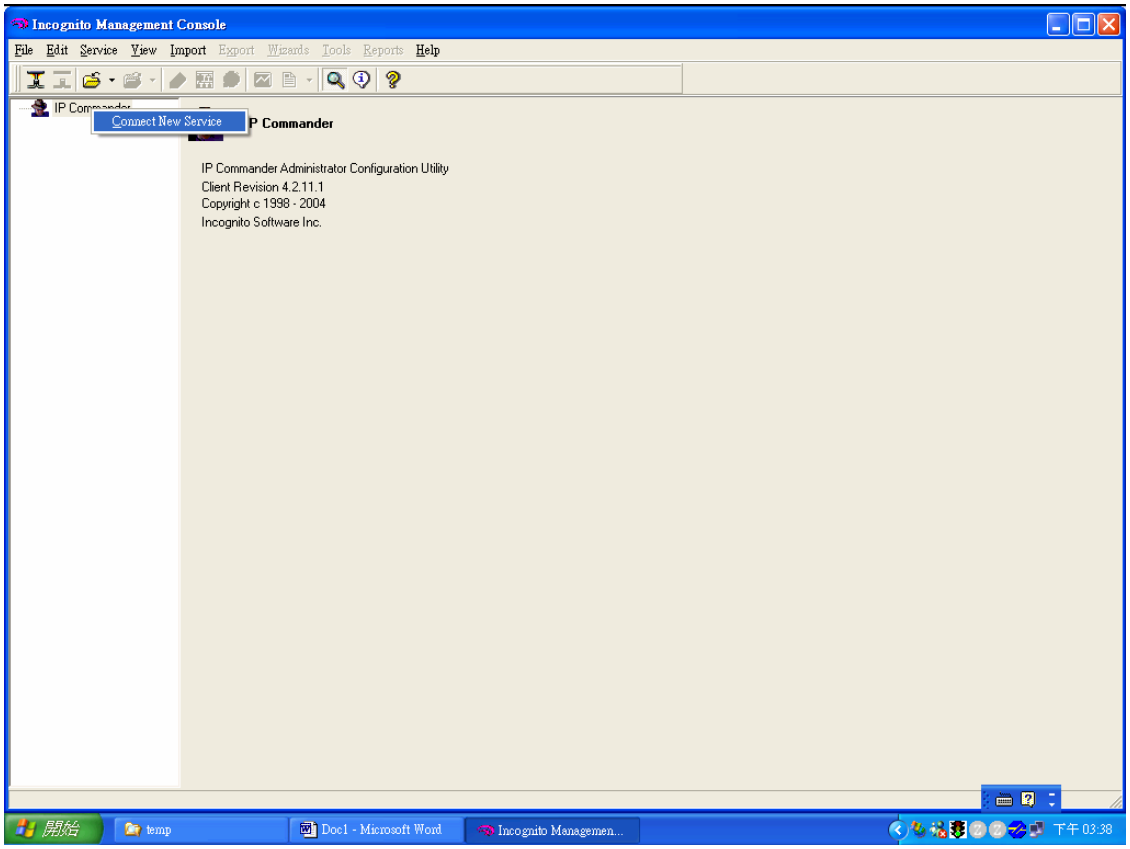


Next connect a computer to the Ethernet port of the CPE to the 1st VDSL port. Refer to the previous application for more information.

2. IP Commander setup

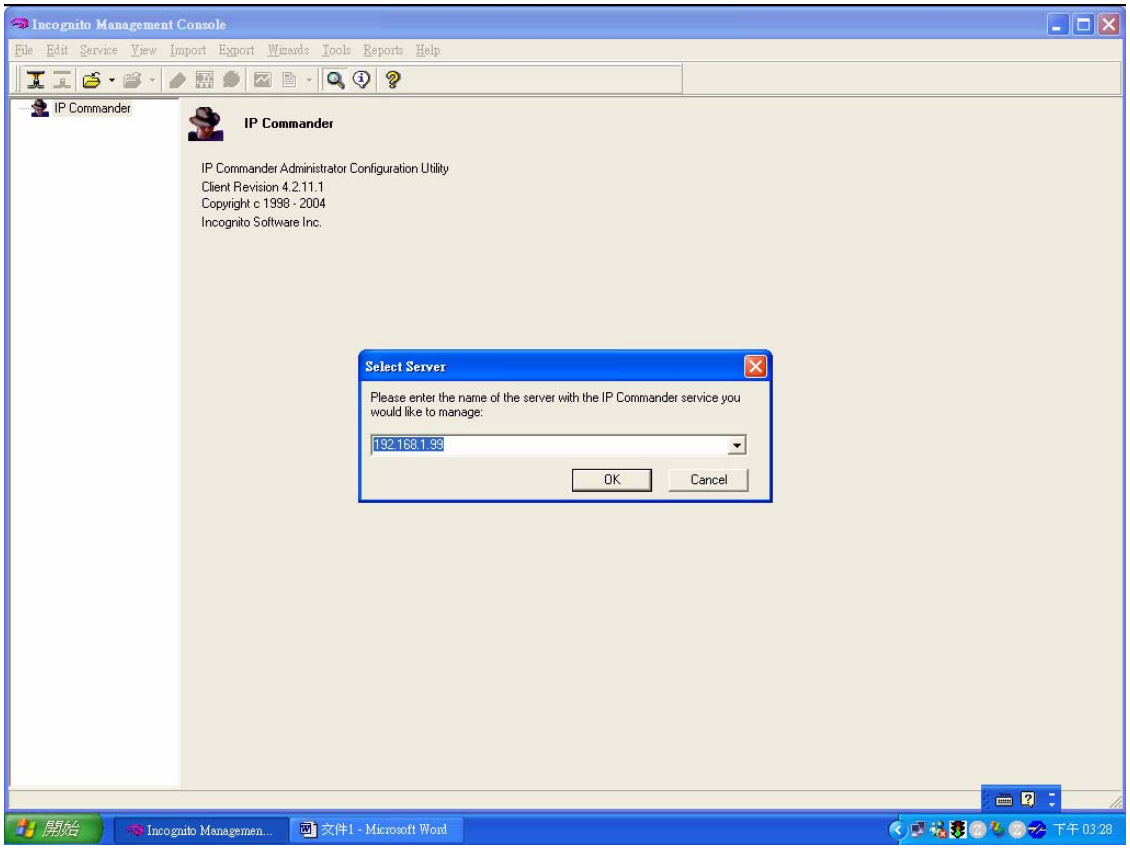
Launch IP Commander and right-click **IP Commander** and click **Connect New Server**.

All contents copyright 2008 ZyXEL Communications Corporation.



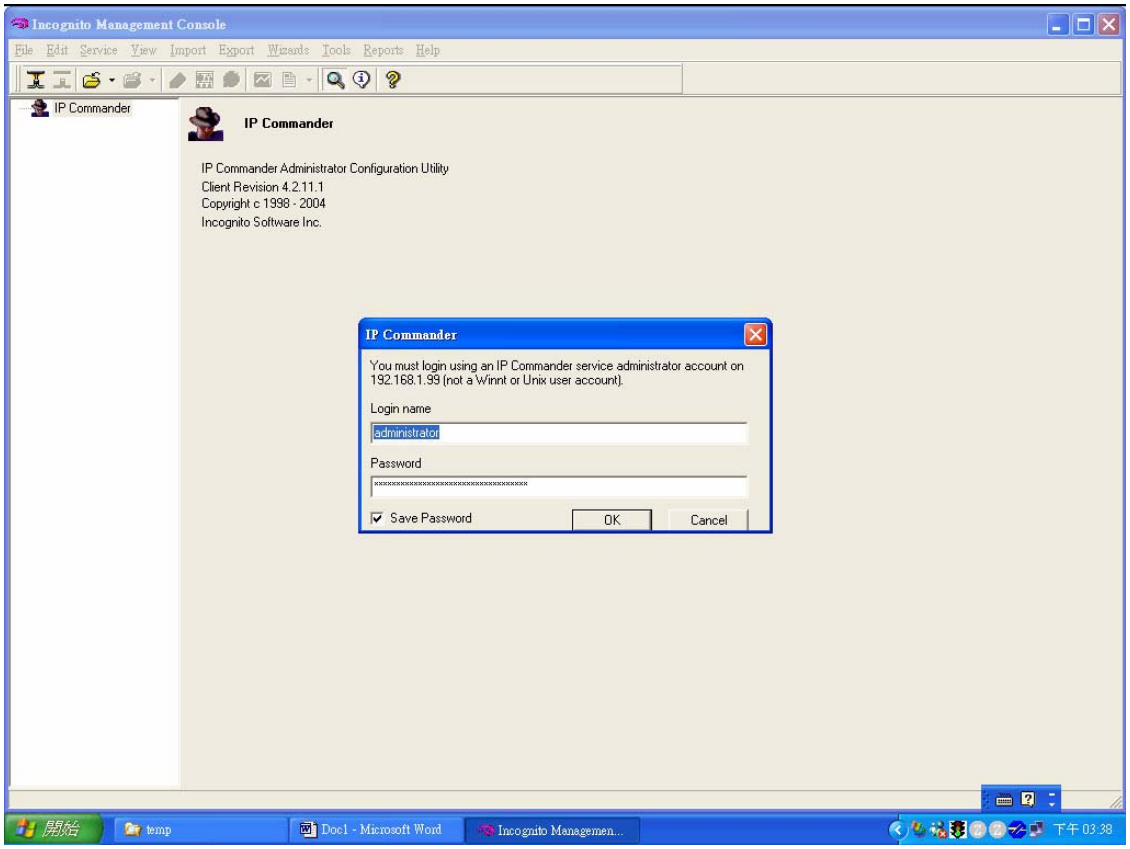
Enter the IP address or domain name for the DHCP server and click **OK**. For this example, we enter 192.168.1.99 for the IP address.

All contents copyright 2008 ZyXEL Communications Corporation.



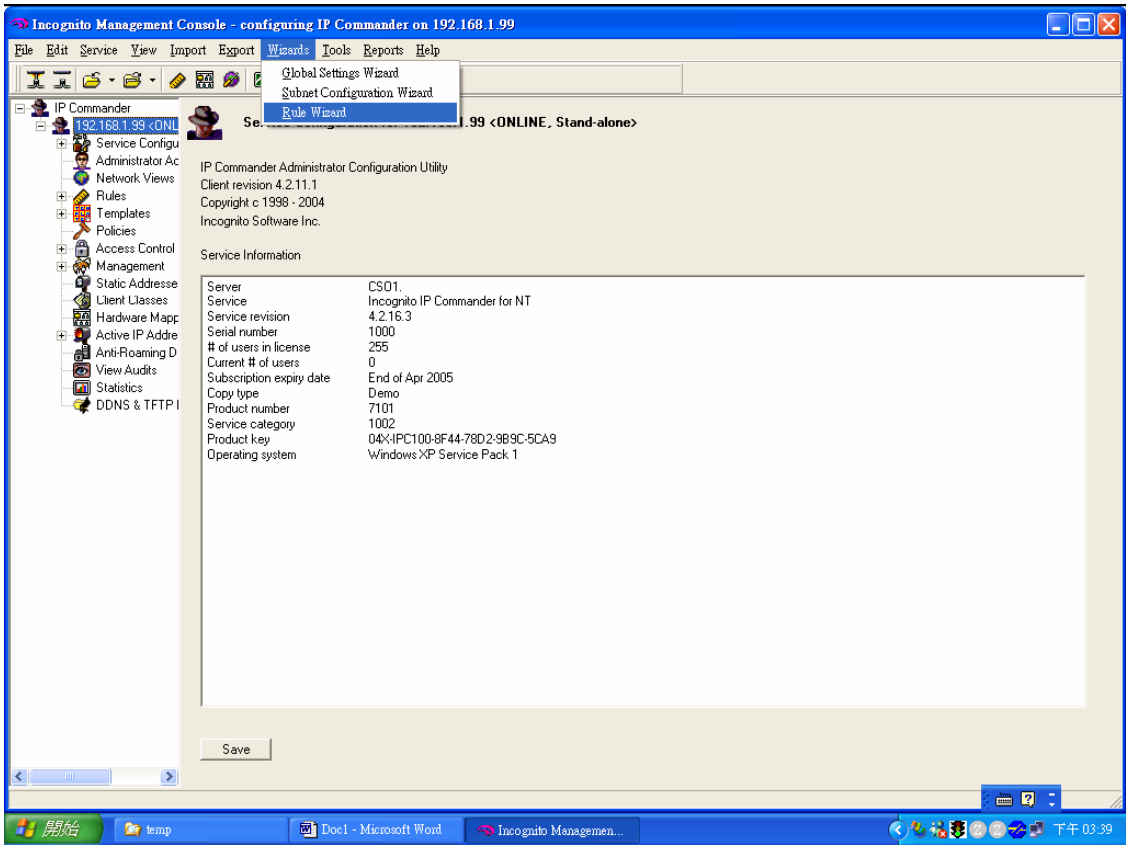
Enter the user name and password. The default user name is “administrator” and password is “incognito”.

All contents copyright 2008 ZyXEL Communications Corporation.



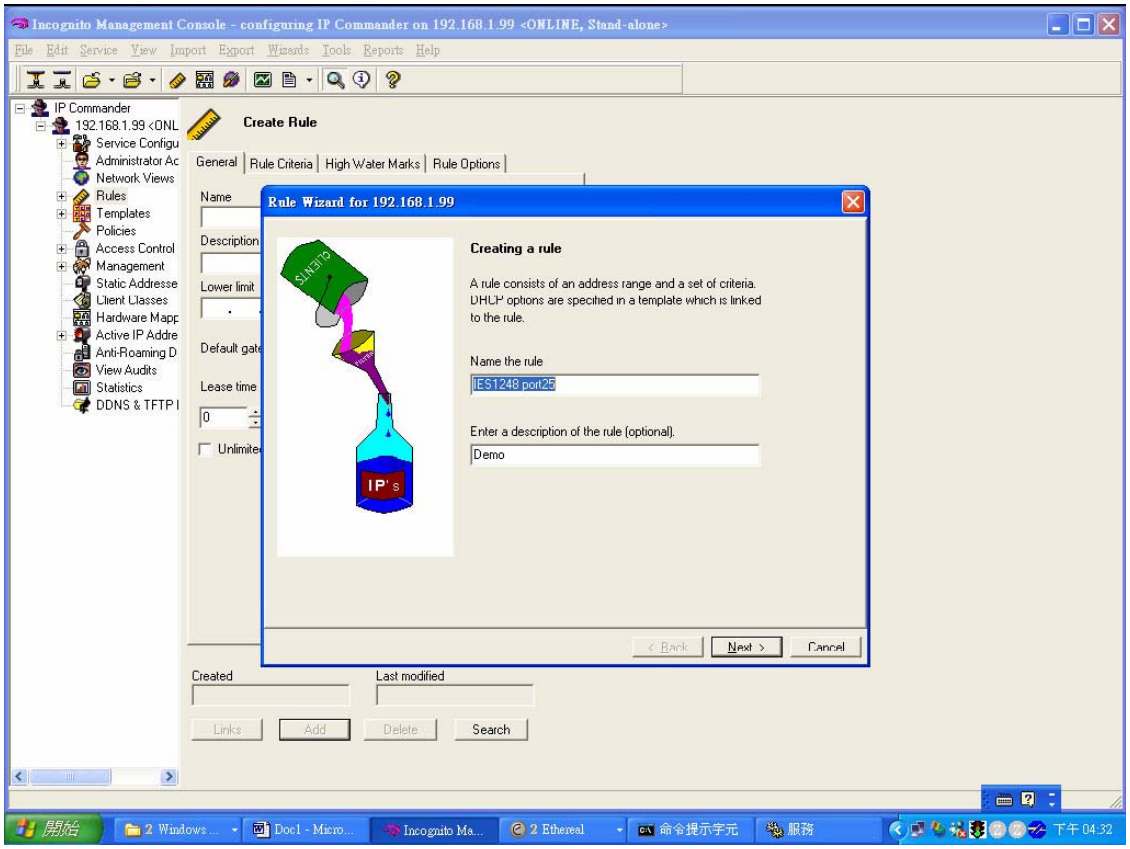
A screen displays. Make sure that the status of your DHCP is **online**. On the top menu, click **Wizard** > **Rule Wizard**.

All contents copyright 2008 ZyXEL Communications Corporation.



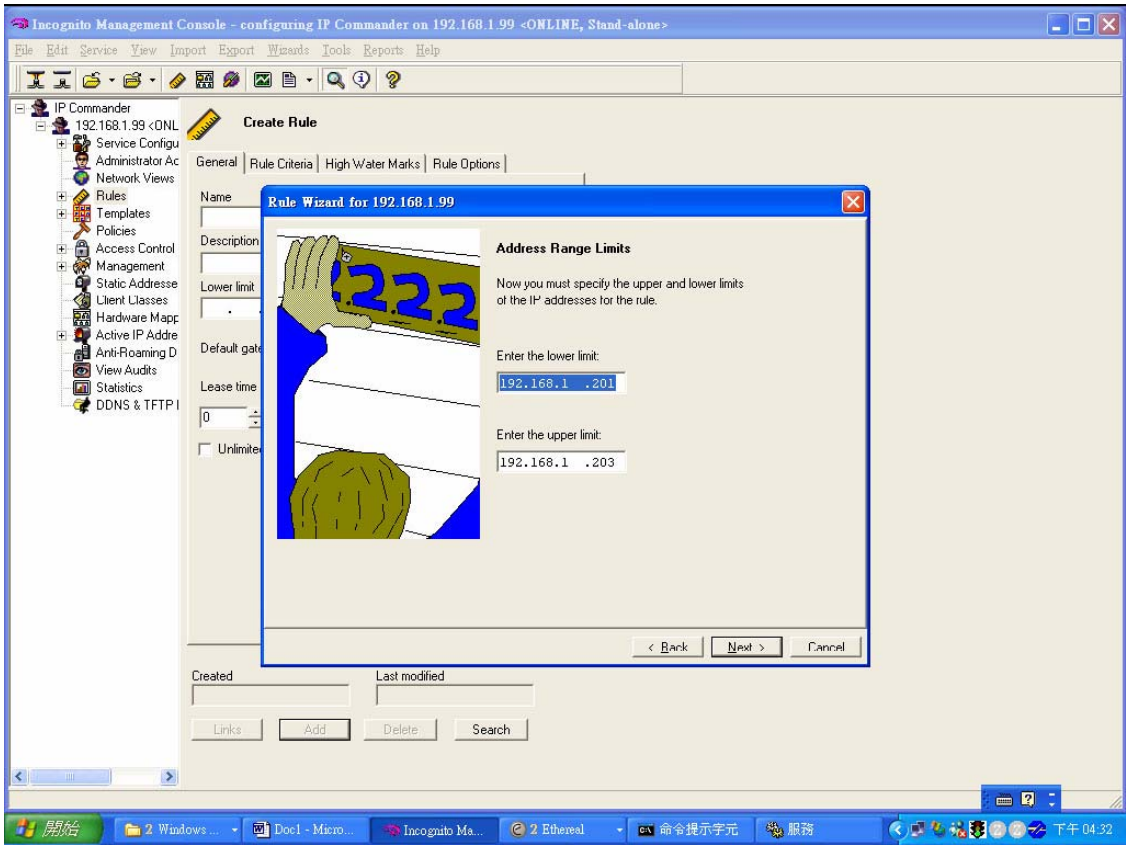
Enter a name and description for the new rule.

All contents copyright 2008 ZyXEL Communications Corporation.


Incognito Management Console - configuring IP Commander on 192.168.1.99 <ONLINE, Stand-alone>
File Edit Service View Import Export Wizards Tools Reports Help
IP Commander
Create Rule
General Rule Criteria High Water Marks Rule Options
Name
Description
Lower limit
Default gate
Lease time
Unlimited
Created
Last modified
Links Add Delete Search
Rule Wizard for 192.168.1.99
Creating a rule
A rule consists of an address range and a set of criteria. DHCP options are specified in a template which is linked to the rule.
Name the rule
IES1248 port25
Enter a description of the rule (optional).
Demo
IP's
< Back Next > Cancel

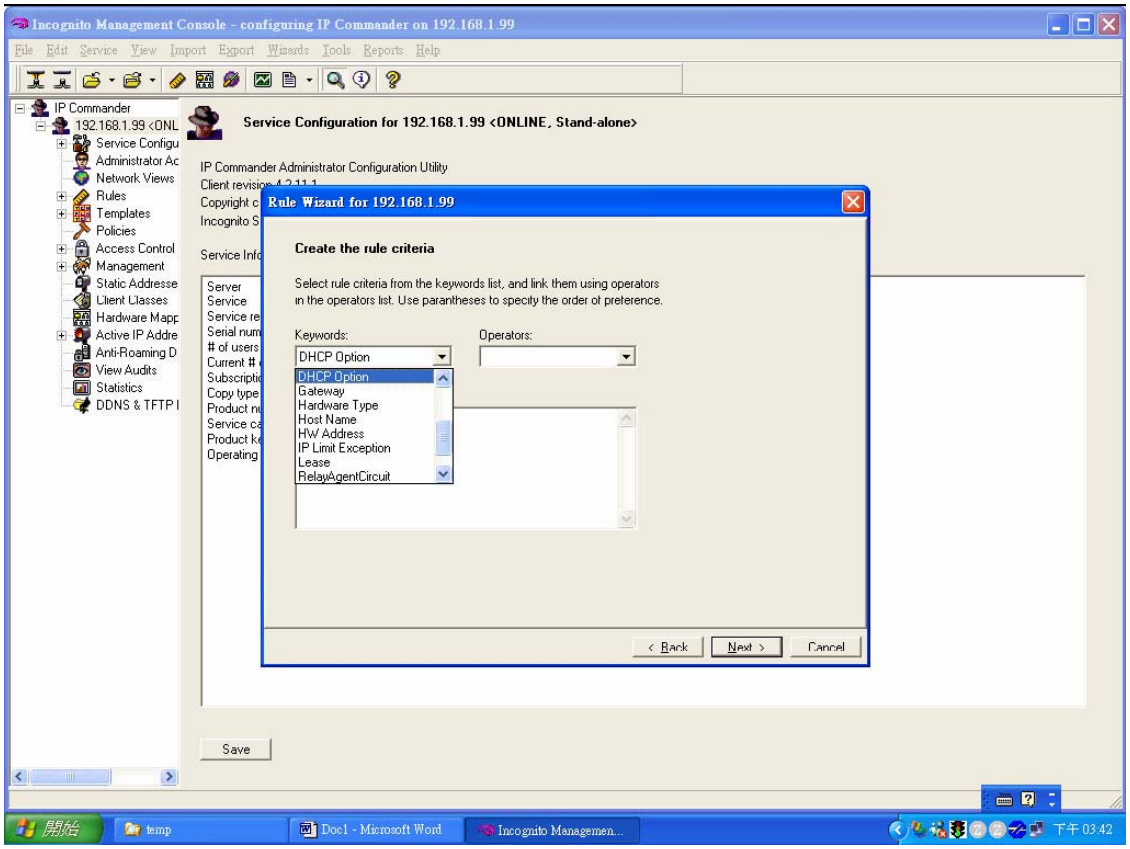
Specify one or a range of IP addresses for this rule. In this example, we configure an IP pool from 192.168.1.201 to 192.168.1.203.

All contents copyright 2008 ZyXEL Communications Corporation.



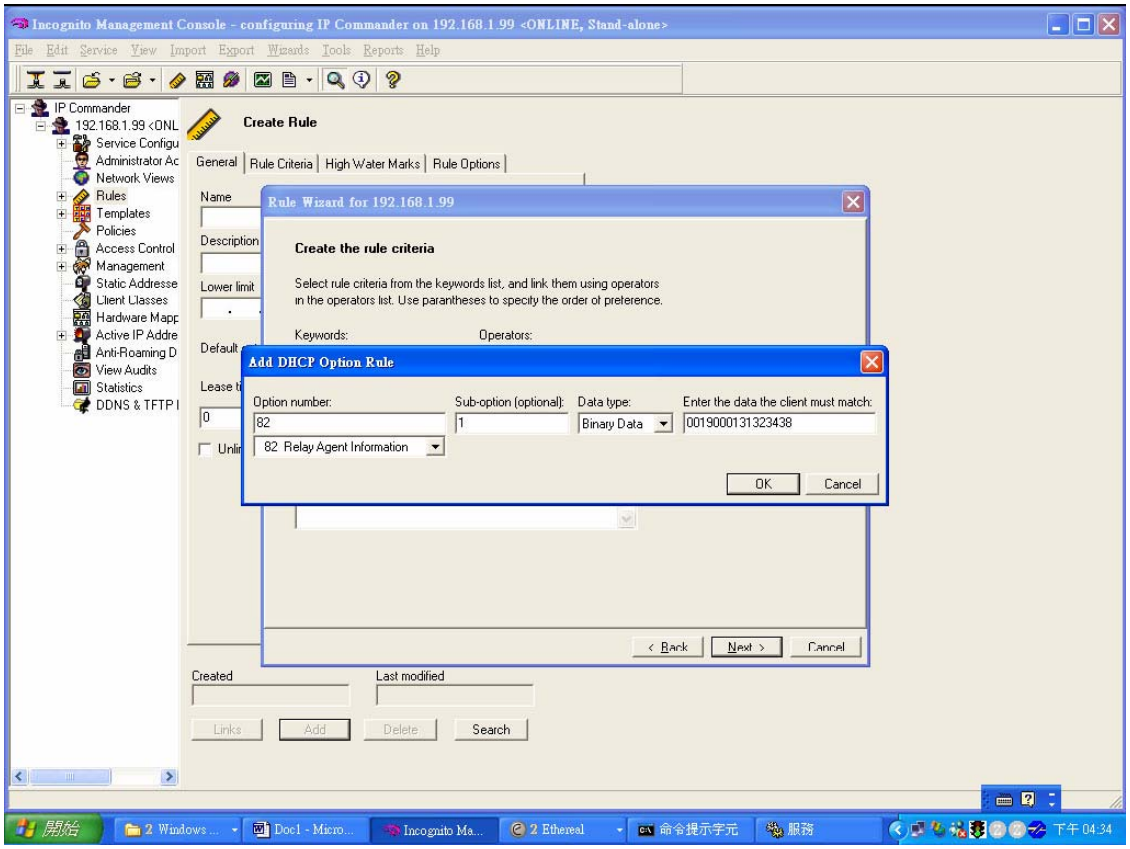
Next select **DHCP Option** in the Keywords field.

All contents copyright 2008 ZyXEL Communications Corporation.



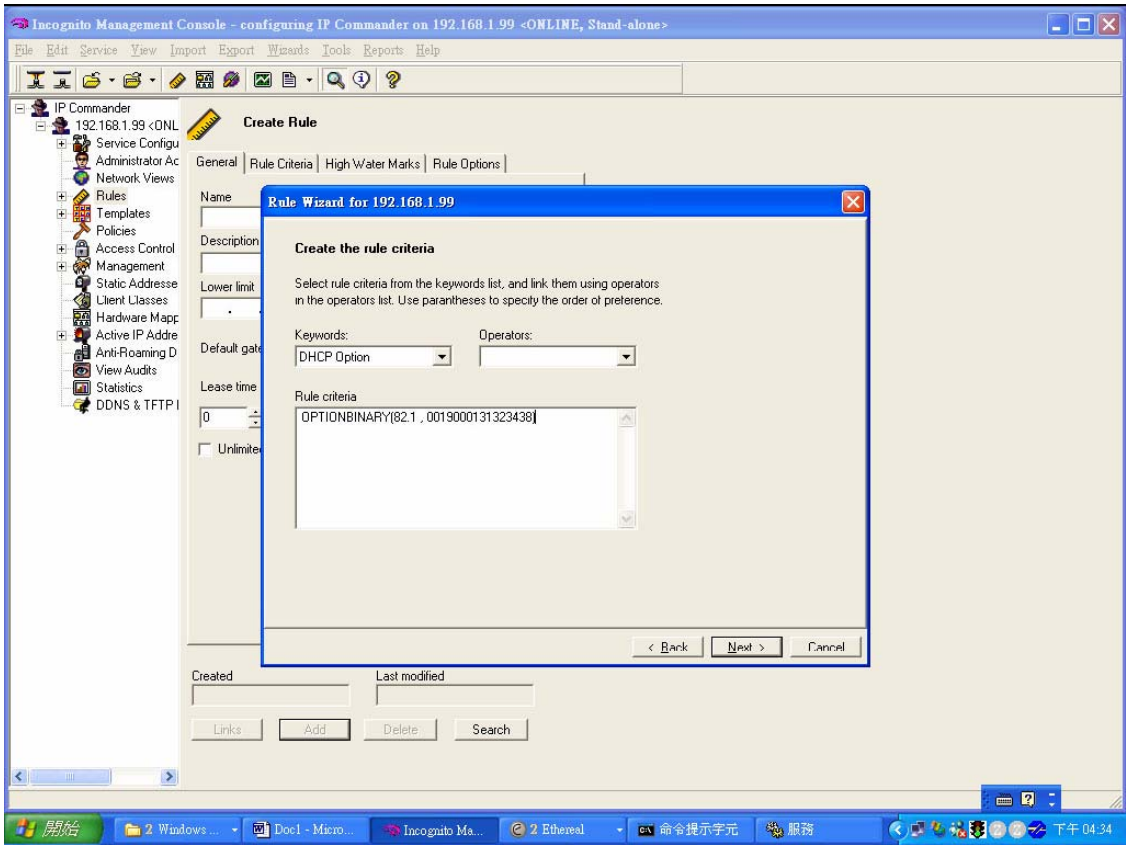
An **Add DHCP Option Rule** screen displays.
Select **Option 82 Relay Agent Information**, set sub-option 1and use binary data. For port 1, VLAN 1 with option82 string of “VES-1616FA-54”, enter “0019000147532d33303132” as the key value and click **OK**. Note that the first two bytes define the port number, the second two bytes is the VLAN ID and the rest of the bytes are the Option 82 string.

All contents copyright 2008 ZyXEL Communications Corporation.



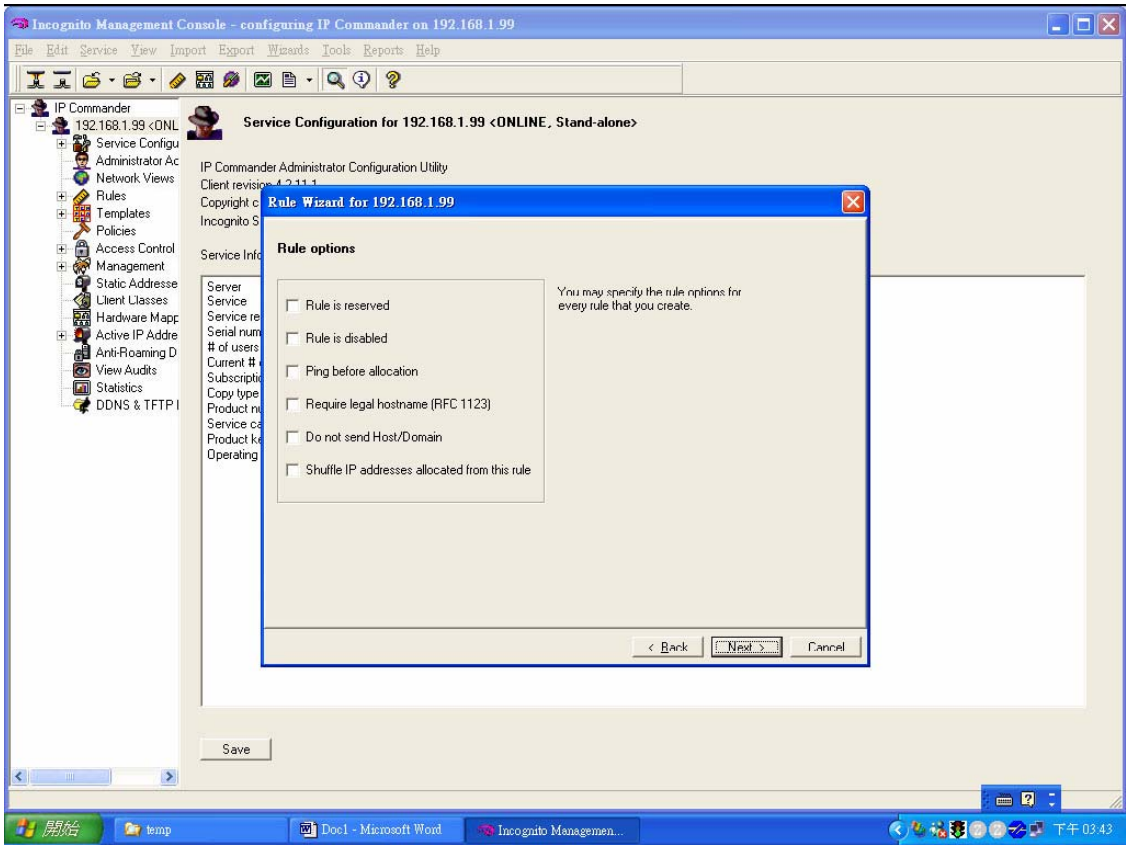
After setting the fields, you should see the following screen.

All contents copyright 2008 ZyXEL Communications Corporation.



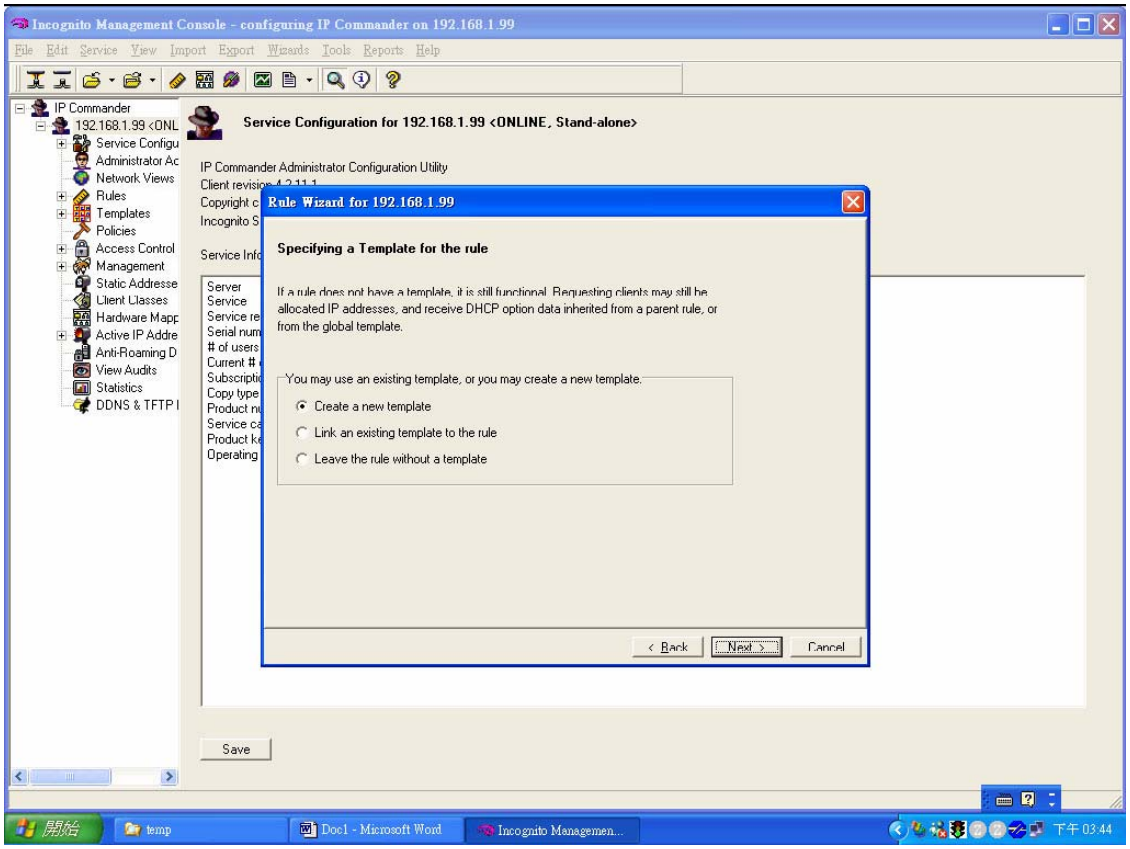
Click **Next** in the screen that displays.

All contents copyright 2008 ZyXEL Communications Corporation.



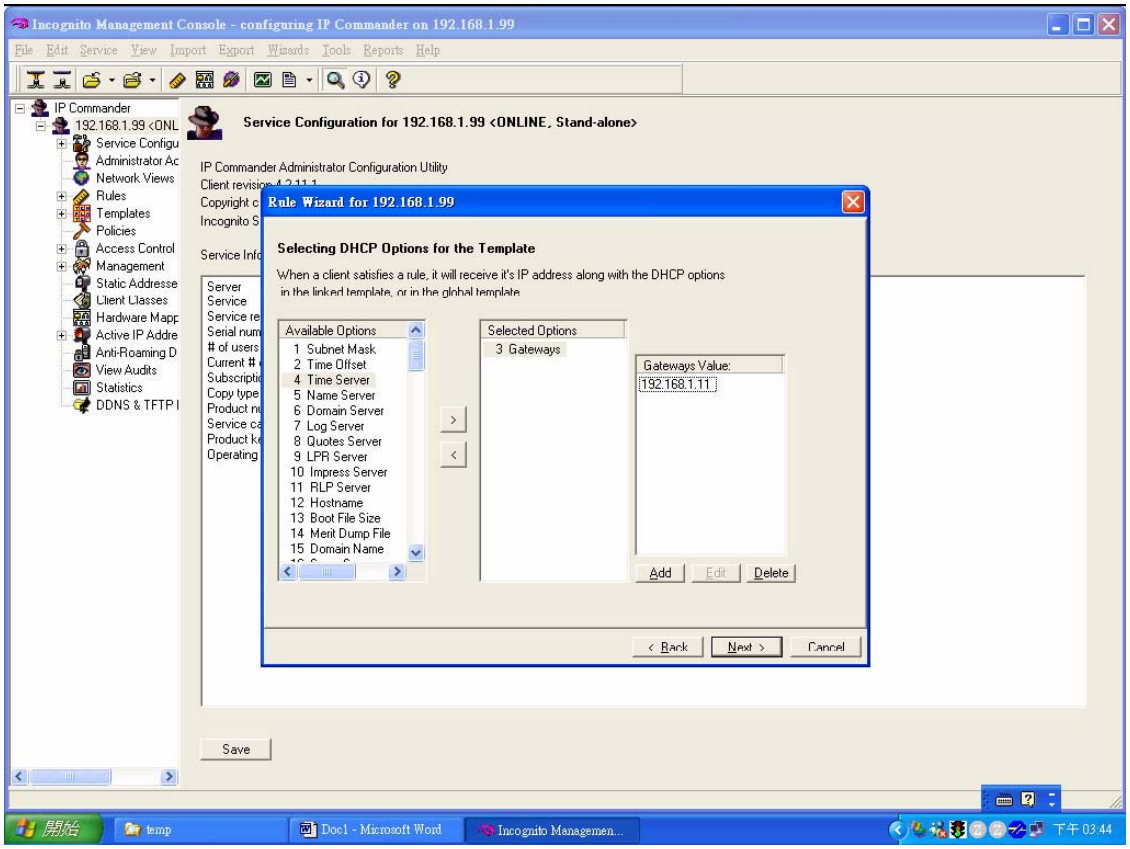
Optionally, you can create a new DHCP template with information such as gateway, DNS server, etc.

All contents copyright 2008 ZyXEL Communications Corporation.



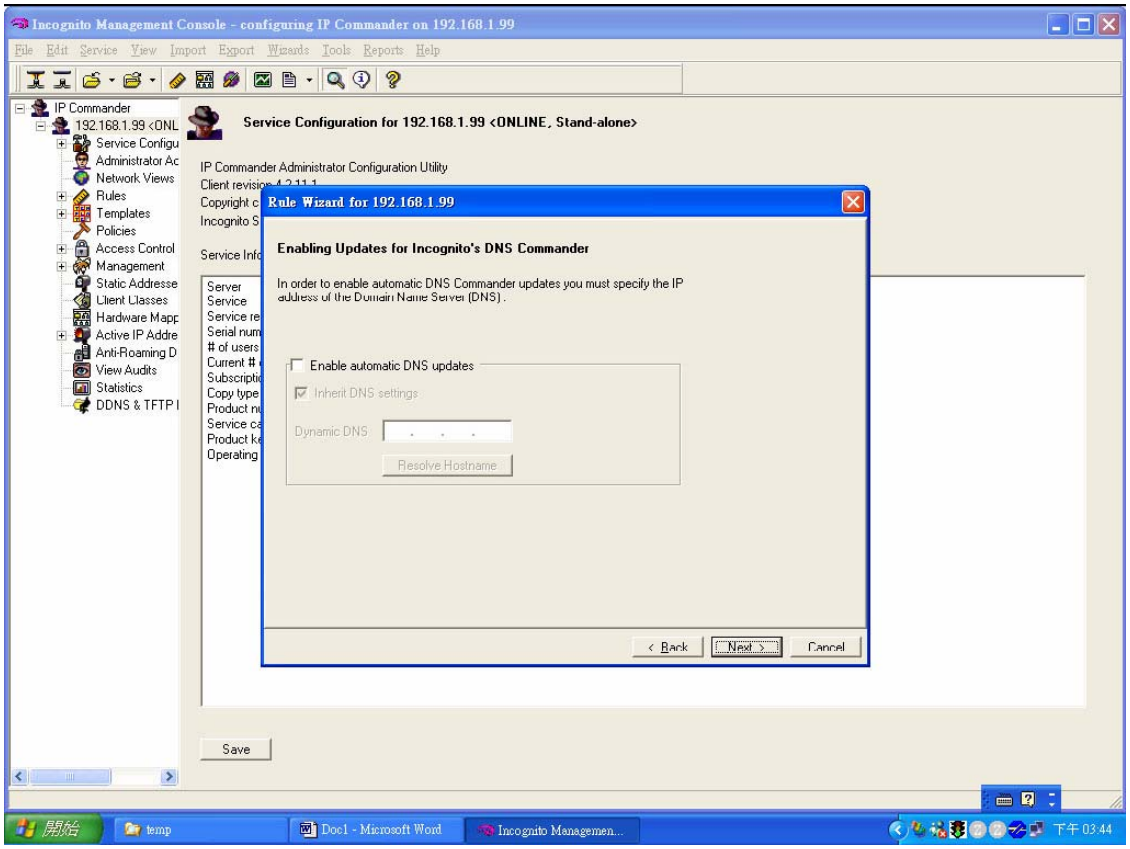
Here, enter “192.168.1.1” as gateway IP address for DHCP clients.

All contents copyright 2008 ZyXEL Communications Corporation.



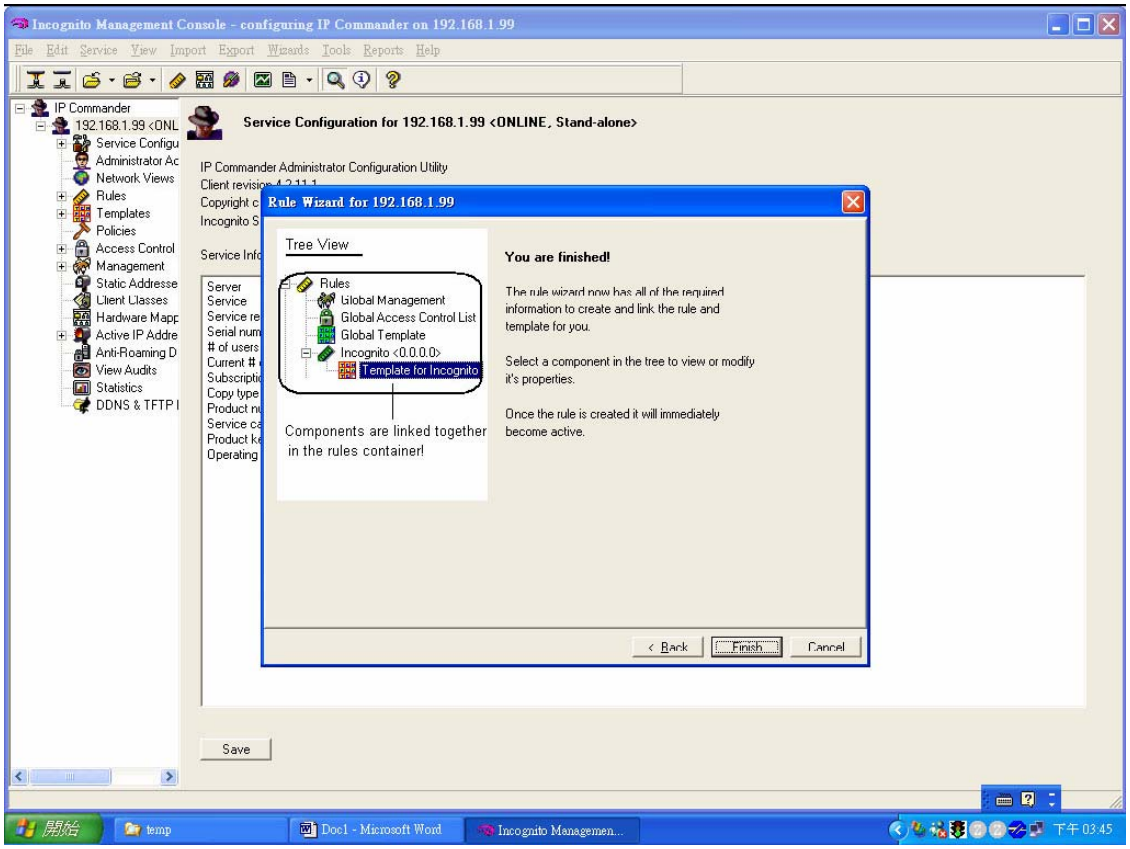
You can choose to enable DDNS service on the DHCP server.

All contents copyright 2008 ZyXEL Communications Corporation.



Click Finish to complete the rule creation.

All contents copyright 2008 ZyXEL Communications Corporation.



After the DHCP server configuration, your computer should be able to get an IP address of 192.168.1.201 when a DHCP request is sent.

Separating a physical network into multiple virtual networks

What is Virtual LAN?

VLAN Overview

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to a group

All contents copyright 2008 ZyXEL Communications Corporation.

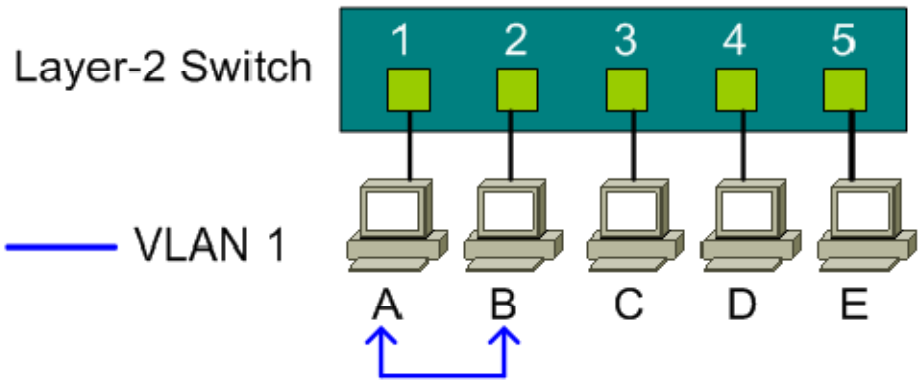
known as the VLAN Group. A station can belong to more than one group. Stations in the same VLAN group can communicate with each other. With VLAN, a station cannot directly communicate with stations that are not in the same VLAN group(s); the traffic must first go through a router.
In GePON applications, VLAN is vital in providing isolation and security among subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN. Thus a user will not see the printers and hard disks of another user in the same building.
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. A VLAN group is a broadcast domain. In traditional Layer-2 switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.
There are two VLAN implementations: Port-based VLAN and IEEE 802.1q Tagged VLAN. VES-1616F-3X supports both VLAN implementations. The major difference between both VLAN implementations is that Tagged VLAN can cross Layer-2 switches but Port-based VLAN cannot.

Port-based VLAN

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port. You must define outgoing ports allowed for each port when using port-based VLANs. Note that VLAN only governs the outgoing traffic. In the other word, it is unidirectional.
Therefore, if you wish to allow two subscriber ports to talk to each other, e.g., between conference rooms in a hotel, you must define the egress (outgoing port) for both ports. An egress port is an outgoing port, that is, a port through which a data packet leaves.
In the following figure, five hosts (A, B, C, D and E) are connected to a 5-port layer-2 switch which supported port-based VLAN.

Case 1:
Hosts A and B can communicate with each other, because they are in the same VLAN group. But Hosts A and B cannot communicate with Hosts C, D, and E.

All contents copyright 2008 ZyXEL Communications Corporation.

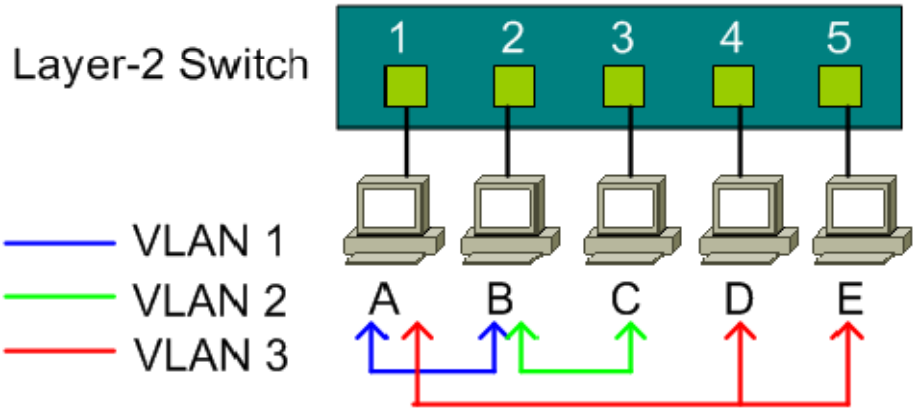


Port-based VLAN definition:

- Egress port for port 1: port 2
- Egress port for port 2: port 1

Case 2:

In this network example, there are three VLAN groups in the physical network. Hosts A and B can communicate with each other since they are in the same VLAN group (VLAN 1). Hosts B and C are in VLAN group 2. Hosts A, D and E are in VLAN group 3.



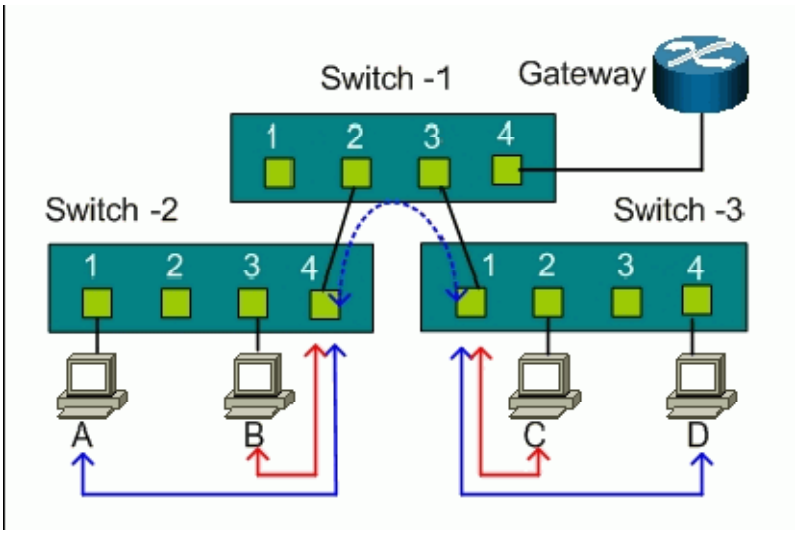
Port-based VLAN definition:

- Egress port for port 1: port 2, port 4, port 5
- Egress port for port 2: port 1, port 3
- Egress port for port 3: port 2
- Egress port for port 4: port 1, port 5
- Egress port for port 5: port 1, port 4

All contents copyright 2008 ZyXEL Communications Corporation.

Port-based VLAN across multiple switches

Port-based VLAN is specific only to the switch on which it was created. Thus, port-based VLAN cannot cross multiple switches. The following figure shows an MTU network example. For network security, subscribers are isolated from each other except for the gateway. There are two switches, Switch-2 and Switch-3, that support port-based VLAN and an uplink to a non-port-based VLAN switch, Switch-1.



For Switch-2, ports 1, 2, and 3 are allowed to communicate with uplink port 4, but not with other ports.

- Switch-2 VLAN 1 member port: port 1 and port 4
- Switch-2 VLAN 2 member port: port 2 and port 4
- Switch-2 VLAN 3 member port: port 3 and port 4

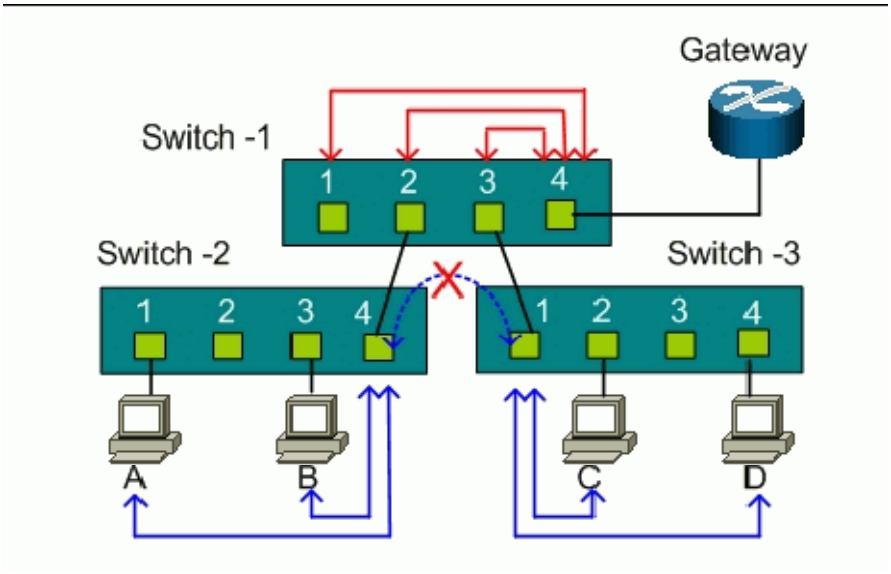
For Switch-3, ports 2, 3, and 4 are allowed to communicate with uplink port 1, but not with other ports.

- Switch-3 VLAN 1 member port: port 2 and port 1
- Switch-3 VLAN 2 member port: port 3 and port 1
- Switch-2 VLAN 3 member port: port 4 and port 1

Host A cannot communicate with Host B due to the port-based VLAN implementation on Switch-2. Host C cannot communicate with Host D due to the port-based VLAN implementation on Switch-3. However, the uplink ports on both Switch-2 and Switch-3 connect to the non- VLAN Switch-1. Hosts A and B is able to communicate with Hosts C and D through the non-VLAN switch because port-based VLAN cannot cross multiple switches.

To provide security between switches, you must install another port-based VLAN switch for the uplink. Each port on the uplink switch also should be separated into different VLANs, except for the port connection to the gateway. So subscribers can only connect to the gateway for Internet access but not communicate with each other.

All contents copyright 2008 ZyXEL Communications Corporation.



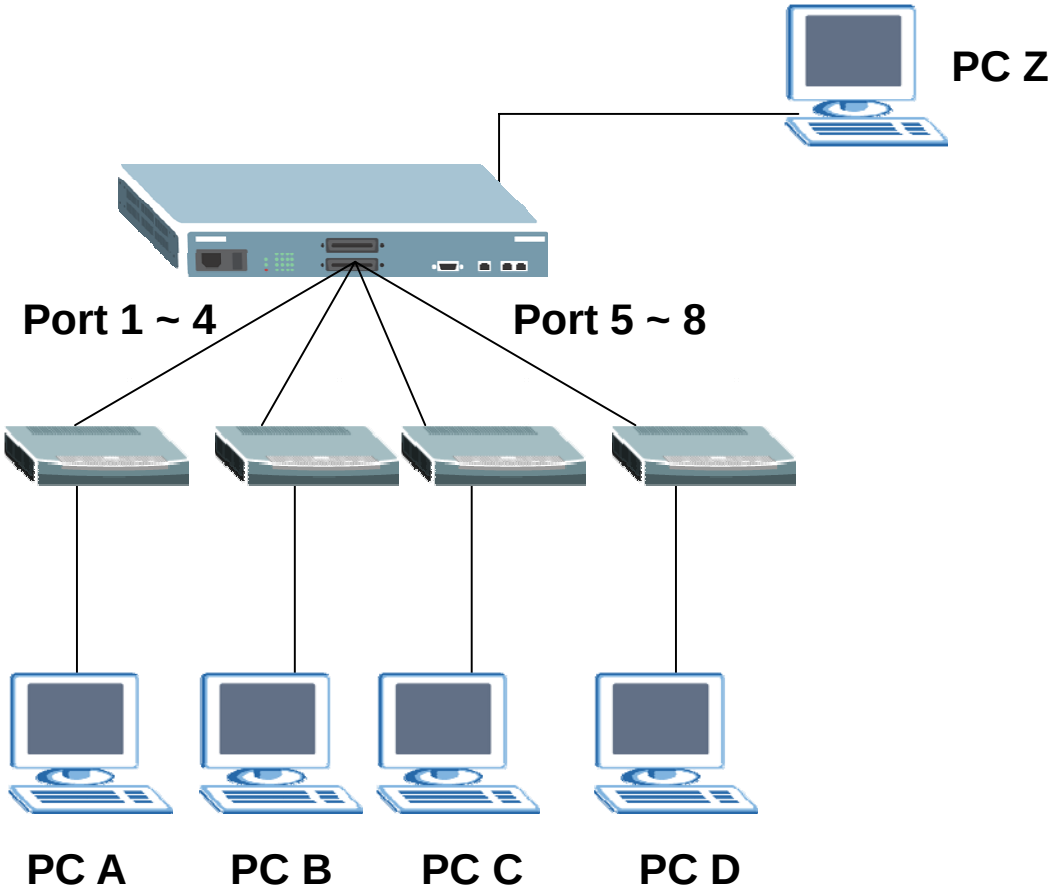
For Switch-1, ports 1, 2, and 3 are allowed to communicate with uplink port 4, but not with other ports.

- Switch-1 VLAN 1 member port: port 1 and port 4
- Switch-1 VLAN 2 member port: port 2 and port 4
- Switch-1 VLAN 3 member port: port 3 and port 4

How to configure Port-Based VLAN

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

All contents copyright 2008 ZyXEL Communications Corporation.



In this scenario, Port Based VLAN is used to separate one physical switch into two smaller logical switches. Ports 1~4 and 17, 18 belong to the same VLAN group, and ports 5~8 are in another group. Port-based VLANs are specific only to the switch on which they were created.

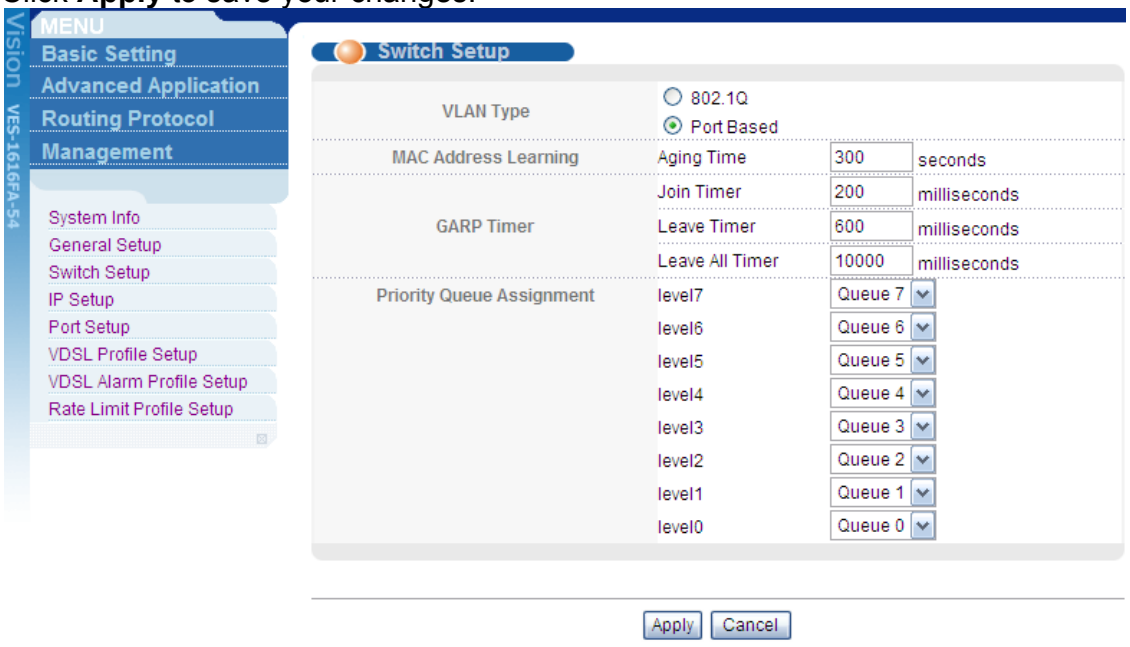
Configuring the Switch Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect a computer to the management port on the switch.
2. By default the management IP address of the switch is 192.168.0.1/24
3. Set the IP settings on your computer to 192.168.0.2/24
4. Open a web browser such as IE and enter http://192.168.0.1 as the URL.
5. When prompted, enter “admin” as the username and “1234” as the password.
6. After you have logged in successfully, the main web configurator screen displays.

All contents copyright 2008 ZyXEL Communications Corporation.

MENU
Basic Setting
Advanced Application
Routing Protocol
Management
Status
VDSL Summary
System Up Time : 26:47:51
Port Net Data Rate State Tx KB/s Rx KB/s Up Time Retrain
1 10.237/10.239M Showtime 0.82 0.0 25:41:24 Retrain
2 0/0 Handshake 0 0 0:00:00 Retrain
3 0/0 Handshake 0 0 0:00:00 Retrain
4 0/0 Handshake 0 0 0:00:00 Retrain
5 0/0 Handshake 0 0 0:00:00 Retrain
6 0/0 Handshake 0 0 0:00:00 Retrain
7 0/0 Handshake 0 0 0:00:00 Retrain
8 0/0 Handshake 0 0 0:00:00 Retrain
9 0/0 Handshake 0 0 0:00:00 Retrain
10 0/0 Handshake 0 0 0:00:00 Retrain
11 0/0 Handshake 0 0 0:00:00 Retrain
12 0/0 Handshake 0 0 0:00:00 Retrain
13 0/0 Handshake 0 0 0:00:00 Retrain
Poll Interval(s) 40 Set Interval Stop Port ALL Clear Counter

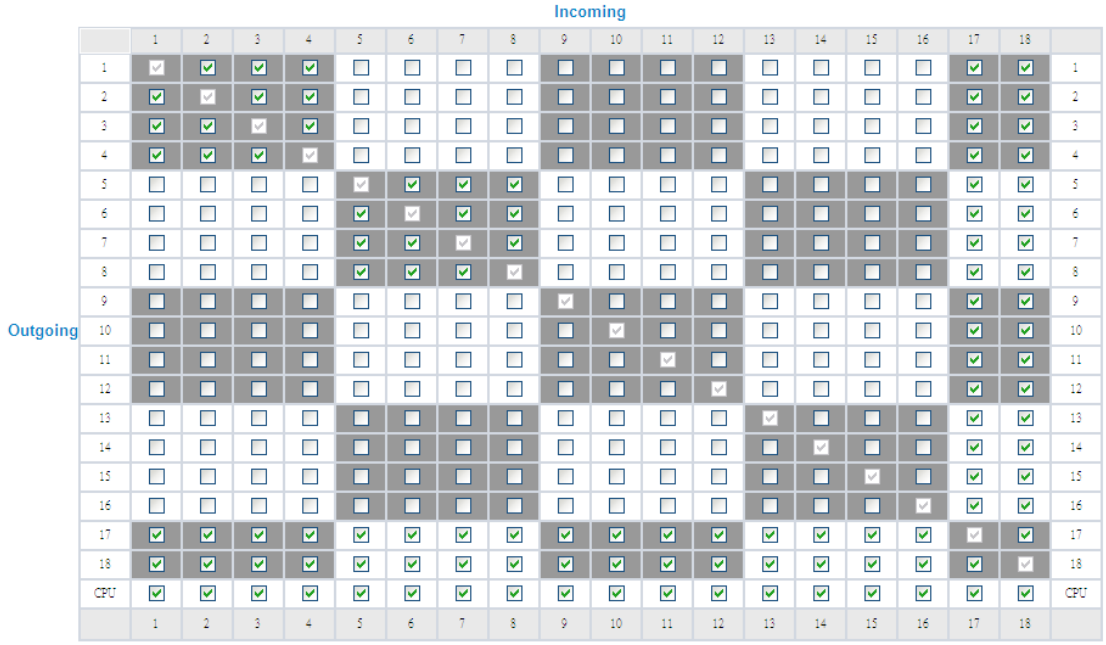
7. First, set the switch to use port based VLAN. Click **Basic Setting > Switch Setup** in the navigation panel and select “Port Based” in the VLAN Type field. Click **Apply** to save your changes.



8. Next create logical partitions on the switch. Click **Advanced Application > VLAN** in the navigation panel and select the ports to belong to the VLAN. For this example, select ports 1~4 and 17, 18 to belong to a VLAN so they can communicate with each other.
Although ports 5~8 are in another group, both groups cannot communicate with each other. Here we also defined ports 17 and 18 as the uplink ports. Therefore,

All contents copyright 2008 ZyXEL Communications Corporation.

both groups can pass data to ports 17 and 18. In another word, these two ports belong to both VLAN groups at the same time. The configuration screen should look similar to the screen as shown.



9. Finally, verify the settings. If you have configured the VLAN settings properly, PC A can ping PC B and PC Z but not PC C or PC D and vice versa.
10. For example,
PC A: 192.168.1.4/24
PC B: 192.168.1.5/24
PC C: 192.168.1.6/24
PC D: 192.168.1.7/24
PC Z: 192.168.1.99/24
11. PING PC B from PC A (successful reply messages)

```
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=12ms TTL=254
Reply from 192.168.1.5: bytes=32 time=6ms TTL=254
Reply from 192.168.1.5: bytes=32 time=7ms TTL=254
Reply from 192.168.1.5: bytes=32 time=6ms TTL=254

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 12ms, Average = 7ms
```

12. PING PC Z from PC A (successful reply messages)

All contents copyright 2008 ZyXEL Communications Corporation.

```
C:\>ping 192.168.1.99

Pinging 192.168.1.99 with 32 bytes of data:

Reply from 192.168.1.99: bytes=32 time=15ms TTL=254
Reply from 192.168.1.99: bytes=32 time=6ms TTL=254
Reply from 192.168.1.99: bytes=32 time=6ms TTL=254
Reply from 192.168.1.99: bytes=32 time=7ms TTL=254

Ping statistics for 192.168.1.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 15ms, Average = 8ms
```

13. PING PC C from PC A (not successful with request timed out message)

```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Configuring the Switch Using the CLI

1. Connect the your computer to the console port on the switch
2. Open your Terminal program (for example, Hyper Terminal in Windows System).
3. Make sure the console connection settings are configured as listed below.
Bps: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None:
4. After you can connect successfully, enter the user name and password.
5. Enter “config” to go into the configuration mode.
6. Enter the following commands to configure Port Based VLAN on your Switch in this network example.

All contents copyright 2008 ZyXEL Communications Corporation.

```
VES-1616FA-54(config)#
VES-1616FA-54(config)# vlan-type port-based interface port-channel 1 no egress s
et 5-8
VES-1616FA-54(config)# vlan-type port-based interface port-channel 2 no egress s
et 5-8
VES-1616FA-54(config)# vlan-type port-based interface port-channel 3 no egress s
et 5-8
VES-1616FA-54(config)#
VES-1616FA-54(config)# vlan-type port-based interface port-channel 4 no egress s
et 5-8
VES-1616FA-54(config)# vlan-type port-based interface port-channel 5 no egress s
et 1-4
VES-1616FA-54(config)# vlan-type port-based interface port-channel 6 no egress s
et 1-4
VES-1616FA-54(config)# vlan-type port-based interface port-channel 7 no egress s
et 1-4
VES-1616FA-54(config)# vlan-type port-based interface port-channel 8 no egress s
et 1-4
VES-1616FA-54(config)# exit
VES-1616FA-54# write memory
```

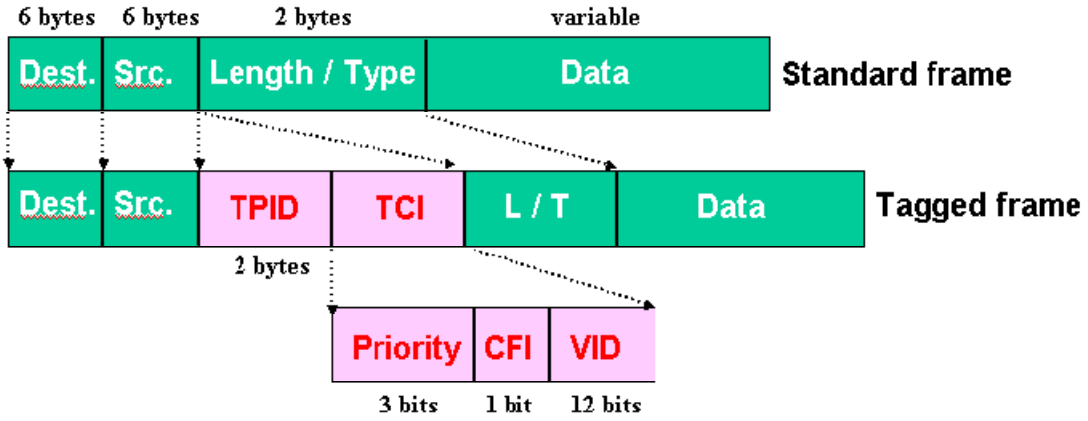
7. After entering the commands, use the “write memory” command under the enable mode to save your configuration.

What is IEEE 802.1Q Tag-based VLAN?

Tag-based VLAN Overview

In the IEEE 802.1Q standard, Tag-based VLAN uses an extra tag in the MAC header to identify the VLAN membership of a frame across bridges. This tag is used for VLAN and QoS (Quality of Service) priority identification. The VLANs can be created statically by an administrator or dynamically through GVRP. The **VLAN ID** associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

All contents copyright 2008 ZyXEL Communications Corporation.

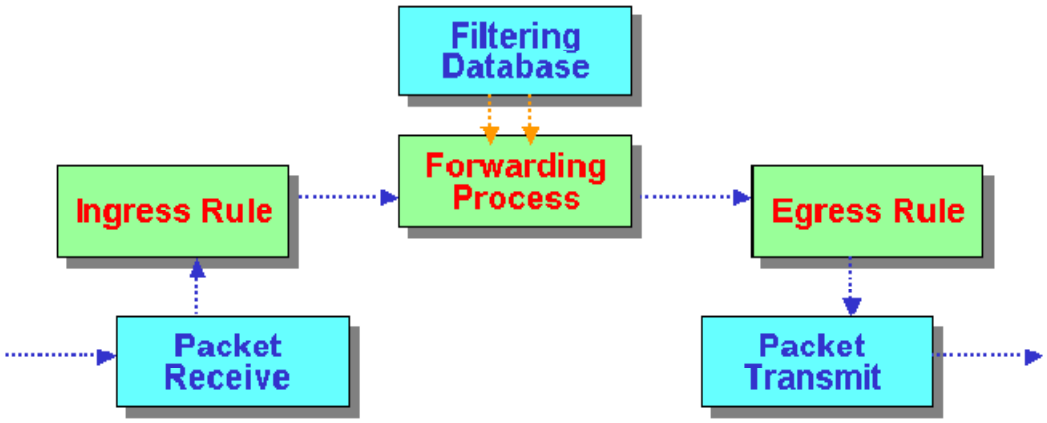


- **TPID:** TPID has a defined value of 8100 in hex. When a frame has the EtherType equal to 8100, this frame carries the IEEE 802.1Q / 802.1P tag.
- **Priority:** The first three bits of the TCI define user priority, giving eight (2^3) priority levels. IEEE 802.1P defines the operation for these 3 user priority bits.
- **CFI:** Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reason between Ethernet type network and Token Ring type network. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- **VID:** VLAN ID is the identification of the VLAN, which is used by the standard 802.1Q. It is 12 bits long and allows the identification of 4096 (2^12) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.
- Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame.

How 802.1Q VLAN works

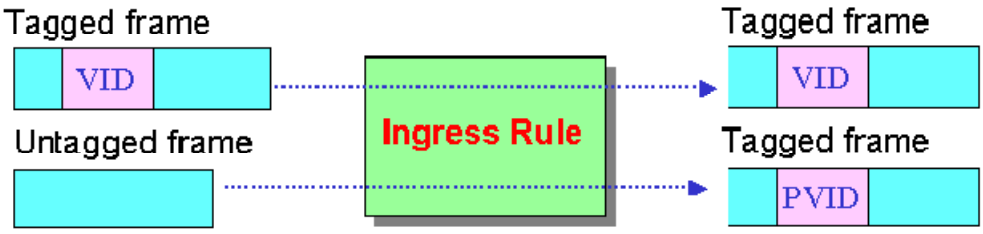
Based on the VID information in the tag, the switch forwards and filters frames on the ports. Ports with the same VID can communicate with each other. IEEE 802.1Q VLAN function defines three tasks: Ingress Process, Forwarding Process and Egress Process.

All contents copyright 2008 ZyXEL Communications Corporation.



1. Ingress Process:
Each port is capable of passing tagged or untagged frames. Ingress Process identifies if the incoming frames contain a tag, and classifies the incoming frames belonging to a VLAN. Each port has its own Ingress rule. If an Ingress rule accepts tagged frames only, the switch will drop all incoming non-tagged frames on the port. If an Ingress rule accepts all frame types, the switch allow both incoming tagged and untagged frames on the port.

When a tagged frame is received on a port, it carries a tag header that has an explicit VID. Ingress Process directly passes the tagged frame to Forwarding Process.
An untagged frame does not carry any VID to which it belongs. When an untagged frame is received, Ingress Process inserts a tag contained the PVID into the untagged frame. Each physical port has a default VID called PVID (Port VID). PVID is assigned to untagged frames or priority tagged frames (frames with null (0) VID) received on this port.



After Ingress Process, all frames have a 4-bytes tag and VID information, and they are transitioned into Forwarding Process.

2. Forwarding Process:
The Forwarding Process makes forwarding decisions on the received frames

All contents copyright 2008 ZyXEL Communications Corporation.

based on the Filtering Database. If you want to allow tagged frames to be forwarded to a certain port, this port must be the egress port of this VID. The egress port is an outgoing port for the specified VLAN, that is, frames with a specified VID tag can go through this port. Filtering Database stores and organizes VLAN registration information useful for switching frames to and from switch ports. It consists of static registration entries (Static VLAN or SVLAN table) and dynamic registration entries (Dynamic VLAN or DVLAN table). SVLAN table is manually added and maintained by the administrator.
DVLAN table is automatically learned via GVRP protocol, and can't be created or updated by the administrator.

VLAN entries in Filtering Database have the following information:
1. **VID:** VLAN ID
2. **Port:** The switch port number
3. **Ad Control:** Registration administration control. There are 3 types of ad control, including **forbidden** registration, **fixed** registration and **normal** registration.
   - **Forbidden** registration: This port is forbidden to be the egress port of the specified VID.
   - **Fixed** registration: While ad control is fixed registration, it means this is a static registration entry. This port is the egress port of the specified VID (a member port of the specified VLAN). Frames with the specified VID tag can go through this port.
   - **Normal** registration: While ad control is normal registration, it means this is a dynamic registration entry. The forwarding decision is depended on the Dynamic VLAN table.
4. **Egress tag Control:** This information is used for Egress Process. The value may be tagged or untagged. If the value is tagged, outgoing frames on the egress port is tagged. If the value is untagged, the tag will be removed before a frame leaves the egress port.

All contents copyright 2008 ZyXEL Communications Corporation.

VID	Port	Ad Control	Tag Control
10	1	Forbidden	Tag
10	2	Fixed	Tag
10	3	Normal	UnTag
20	1	Fixed	Tag
20	5	Fixed	UnTag

Filtering Database

VID	Egress Port
10	1
10	2
20	3

Dynamic VLAN (DVLAN) table

3. Egress Process:
The Egress Process decides if the outgoing frames are to be sent tagged or untagged. The Egress Process refers to the egress tag control information in Filtering Database. If the value is tagged, outgoing frames on the egress port is tagged. If the value is untagged, the tag will be removed before a frame leaves the egress port.

Connecting Two Switches using VLAN

This example shows you how to configure VLAN settings on two VES-1616FA-54 switches which are connected using the Ethernet port. There are five VLANs on the first switch and seven VLANs on the second switch. The Ethernet port is port 17 on both switches. VLANs are configured on the switches but how to configure port 17 as the trunk port on both switches?
The following figure shows this network example.

All contents copyright 2008 ZyXEL Communications Corporation.

The VLAN configurations on the two switches are as follows:
VLAN 101, 102, 103, 104, 105, 106, 107 on switch A
VLAN 101, 102, 103, 104, 105, on switch B
1. VLAN Configuration on switch A

VLAN Status
The Number Of VLAN = 9

VLAN Port Setting Static VLAN

Index	VID	Port Number									Elapsed Time	Status
		2	4	6	8	10	12	14	16	18		
		1	3	5	7	9	11	13	15	17		
1	1	U	U	U	U	U	U	U	U	U	0:00:19	Static
		U	U	U	U	U	U	U	U	U		
2	101	U	-	-	-	-	-	-	-	-	0:00:18	Static
		U	-	-	-	-	-	-	-	T		
3	102	-	U	-	-	-	-	-	-	-	0:00:18	Static
		-	U	-	-	-	-	-	-	T		
4	103	-	-	U	-	-	-	-	-	-	0:00:18	Static
		-	-	U	-	-	-	-	-	T		
5	104	-	-	-	U	-	-	-	-	-	0:00:18	Static
		-	-	-	U	-	-	-	-	T		
6	105	-	-	-	-	U	-	-	-	-	0:00:18	Static
		-	-	-	-	U	-	-	-	T		
7	106	-	-	-	-	-	U	-	-	-	0:00:18	Static
		-	-	-	-	-	U	U	-	T		
8	107	-	-	-	-	-	-	U	U	-	0:00:18	Static
		-	-	-	-	-	-	-	U	T		

2. VLAN Configuration on switch B

All contents copyright 2008 ZyXEL Communications Corporation.

Answer:

In switch A, add port 17 in each VLAN
VID:101 (port 1,2,"17 TAG")
VID:102 (port 3,4,"17 TAG")
VID:103 (port 5,6,"17 TAG")
VID:104 (port 7,8,"17 TAG")
VID:105 (port 9,10,"17 TAG")
VID:106 (port 11,12,13,"17 TAG")
VID:107 (port 14,15,16,"17 TAG")

In switch B, add port 17 in each VLAN
VID:101 (port 1,2,3,"17 TAG")
VID:102 (port 4,5,6,"17 TAG")
VID:103 (port 7,8,9,"17 TAG")
VID:104 (port 10,11,12,"17 TAG")
VID:105 (port 13,14,15,16,"17 TAG")
Clients in the same VLAN on both switches can communicate with each other.
PVID:
Set PVID on switch A
Port 1, 2 : **101**
Port 3, 4 : **102**
Port 5, 6 : **103**
Port 7, 8 : **104**
Port 9, 10 : **105**
Port 11, 12, 13 : **106**
Port 14, 15, 16 : **107**
port 25: PVID=any
Set PVID on switch B:

All contents copyright 2008 ZyXEL Communications Corporation.

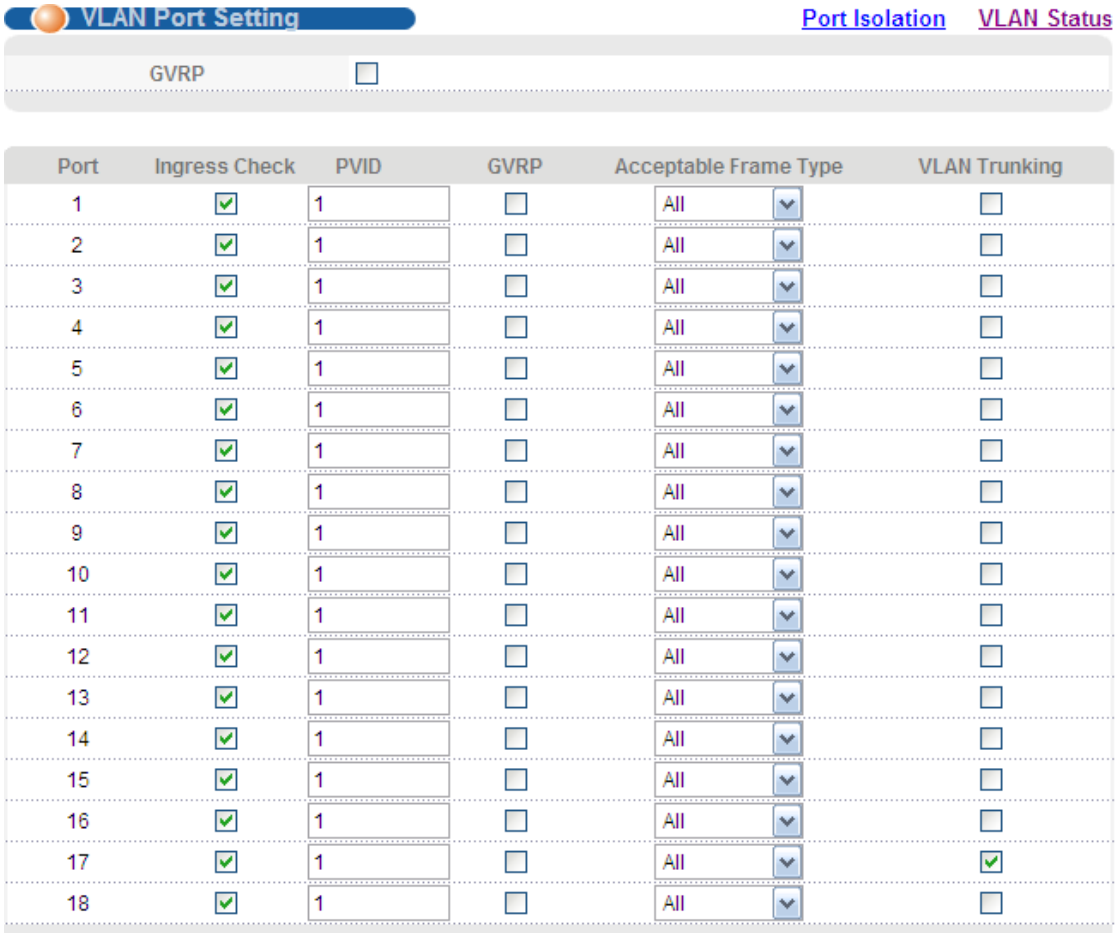
Port 1, 2, 3 : **101**
Port 4, 5, 6 : **102**
Port 7, 8, 9 : **103**
Port 10, 11, 12 : **104**
Port 13, 14, 15, 16 : **105**
Port 25:PVID=any

Setting up VLAN Trunking

With the benefit of deploying VLAN trunking, you can connect two switches through a port that is configured as the VLAN trunking port. VLAN tagged frames from PC1 connected to switch 1 can reach PC 2 connected to switch 2 through the VLAN trunking port. In this example, port 17 on VES 1 is configured as the VLAN Trunking port while on VES 2, port 17 is the VLAN Trunking port.
The following figure shows the network example.

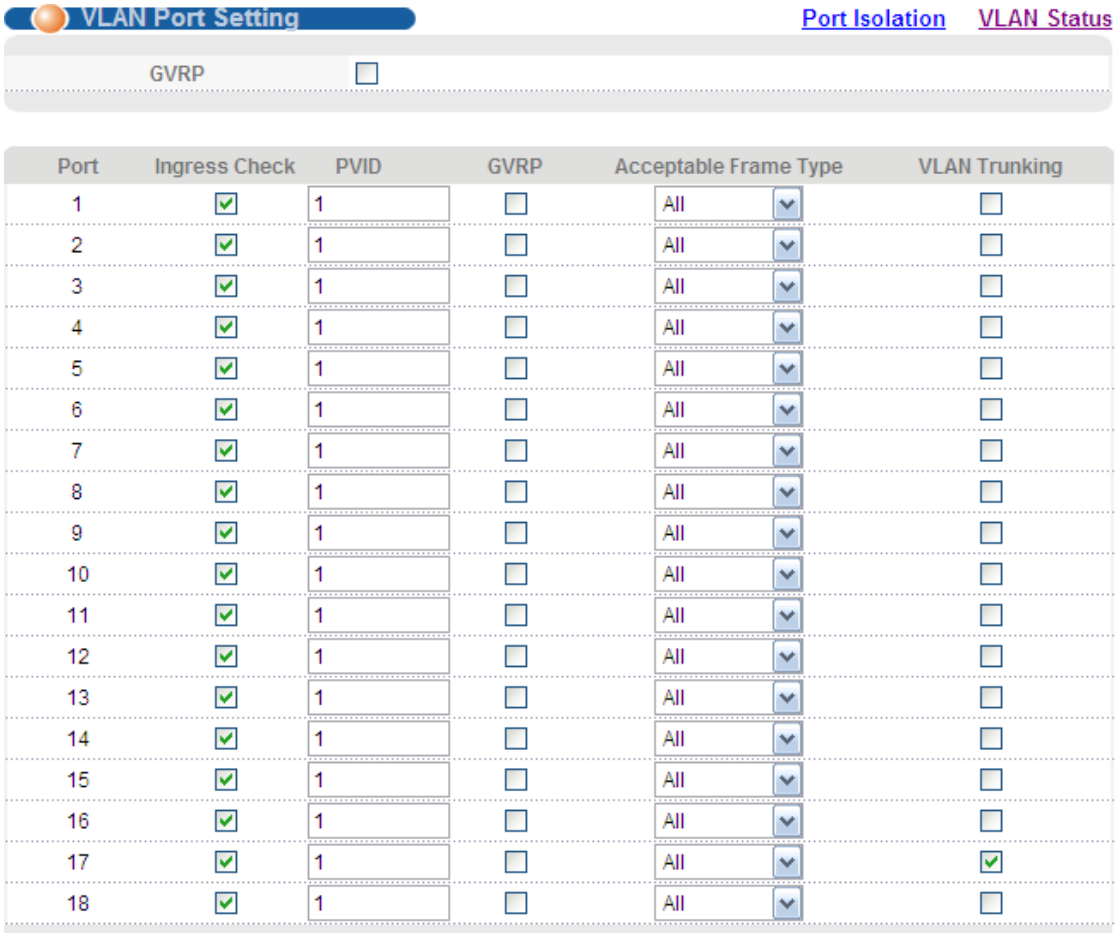
The configuration screen for switch 1 is shown as follows.

All contents copyright 2008 ZyXEL Communications Corporation.



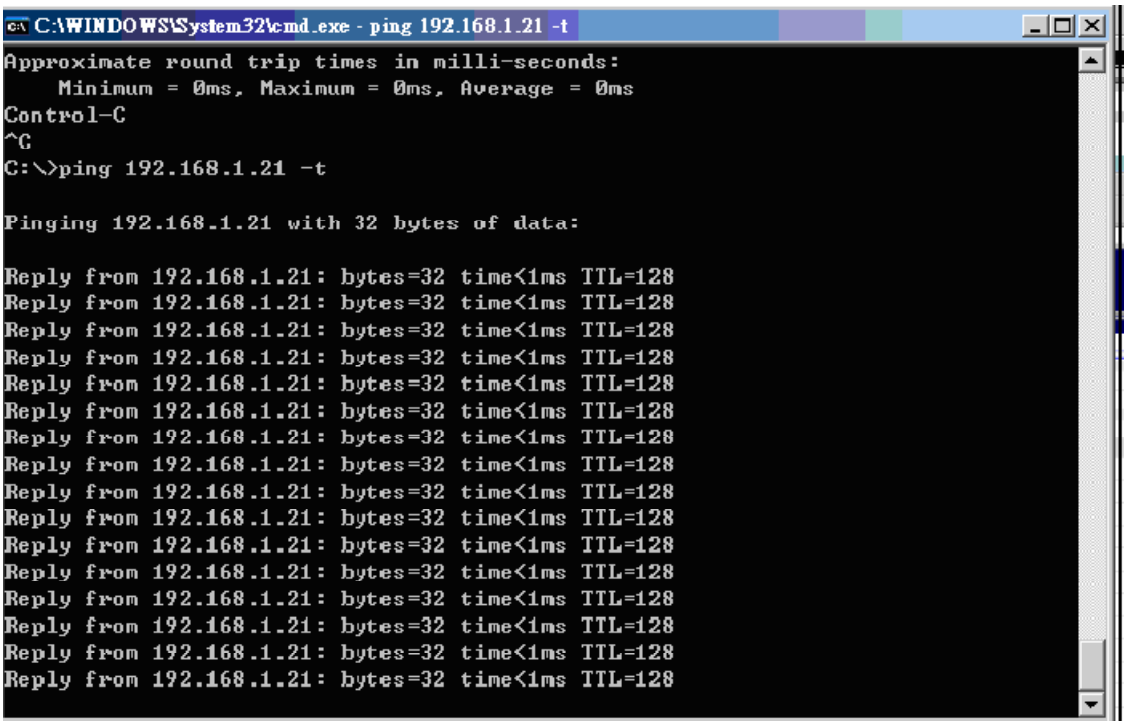
The configuration screen for switch 2 is shown as follows.

All contents copyright 2008 ZyXEL Communications Corporation.



In the VES 1, we set port 1 as VLAN 2 untag
In the VES 2, we set port 2 as VLAN 2 untag.
The switch 1 IP address: 192.168.1.31
The switch 2 IP address: 192.168.1.21
After the configuration, you can see that PC 1 connected to port 2 on switch 1 can still ping PC 2 connected to port 6 on switch 2.

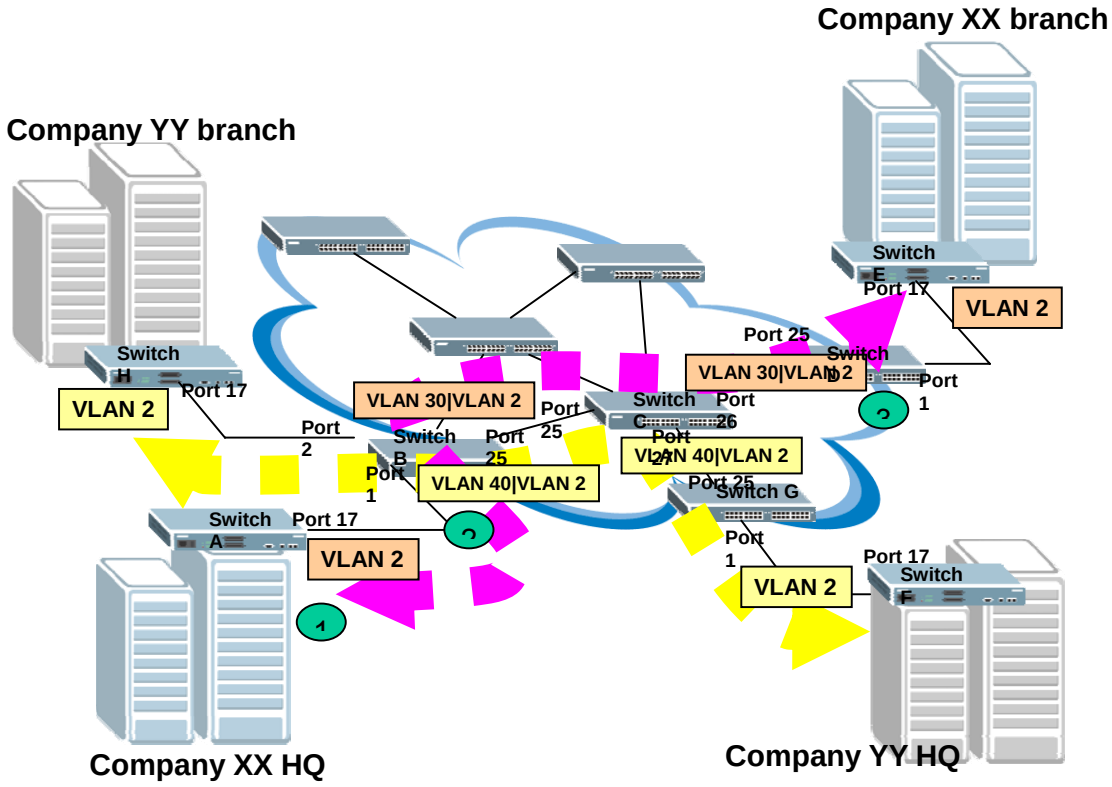
All contents copyright 2008 ZyXEL Communications Corporation.



All contents copyright 2008 ZyXEL Communications Corporation.

VLAN Stacking Overview

VLAN stacking allows a carrier to offer multiple virtual LANs over a single circuit. In essence, the carrier creates an Ethernet VPN to tunnel customer VLANs across its WAN. Thus it helps to avoid name conflicts among customers of multiple service providers who connect to the same carrier.
VLAN stacking works by assigning two VLAN IDs to each frame header. One is a "backbone" VLAN ID used by the service provider, the other (up to 4,096 unique 802.1Q VLAN tags) is used by the customers.
The following figure shows a network example.



In this example, company XX and company YY both subscribe to the same ISP for Internet service. Both companies have an internal VLAN group with VID 1. In order to prevent VLAN-tagged packets between these two companies from transmitting to each other's network, VLAN stacking is implemented in the ISP's network. The ISP assigns a service provider VID for each company- company XX is assigned an SP VID of 30 and company YY is assigned an SP VID of 40.

The following shows the packet flow between **Company XX HQ** and **its branch**

All contents copyright 2008 ZyXEL Communications Corporation.

office.
Company XX HQ → Switch A → Switch B → Switch C → Switch D → Company XX Branch Office.
In this case, VLAN Stacking is enabled on access ports 11 and 12 on Switch B. An SP tag is appended for ingress traffic and the appended SP tagged is removed during egress. VLAN Stacking is also enabled on the tunnel port on switches B (port 10), C, and D. Static VLAN Tx tagging must be DISABLED for the port which is set as a Normal or Access Port. Static VLAN Tx Tagging MUST be enabled on a port set as the Tunnel port.

The following shows the packet flow between **Company YY HQ** and **its branch office**.
Company YY HQ → Switch F → Switch G → Switch C → Switch B → Switch H → Company YY Branch Office.
VLAN Stacking is enabled on access port 10 on Switch G. An SP tag is appended on the ingress traffic and the SP tag is removed during egress. VLAN Stacking is enabled on a Tunnel port on switches G (port 9), C, and B.

From Switch A to Switch H
Switch A:
Enabled VLAN, VLAN1 and egress tagging on Port 17
Port 1 is connected to another access switch in a building.
Port 17 is connected to port 11 on Switch B
Switch B:
Enabled VLAN Stacking and STP
Port 1 is connected to port 17 on Switch A
Port 2 is connected to port 17 on Switch H
Port 25 is connected to port 25 Switch C
Switch C:
Enabled VLAN Stacking and STP
Port 27 is connected to port 25 on Switch G
Port 26 is connected to port 25 on Switch D
Port 25 is connected to port 25 on Switch B
Switch D:
Enabled VLAN Stacking
Port 1 is connected to port 17 on Switch E
Port 25 is connected to port 26 on Switch C
Switch E:
Enabled VLAN, VLAN1, and egress tagging on Port 17
Port 1 is connected to another access switch in the building.
Port 17 is connected to port 1 on Switch D
Switch F:
Enabled VLAN, VLAN1, and egress tagging on Port 17
Port 1 is connected to another access switch in the building.
Port 17 is connected to port 1 on Switch G
Switch G:

All contents copyright 2008 ZyXEL Communications Corporation.

Enabled VLAN Stacking
Port 1 is connected to port 17 on Switch F
Port 25 is connected to port 27 on Switch C
Switch H:
Enabled VLAN, VLAN1, and egress tagging on Port 17
Port 1 is connected to another access switch in the building.
Port 17 is connected to port 2 on Switch B

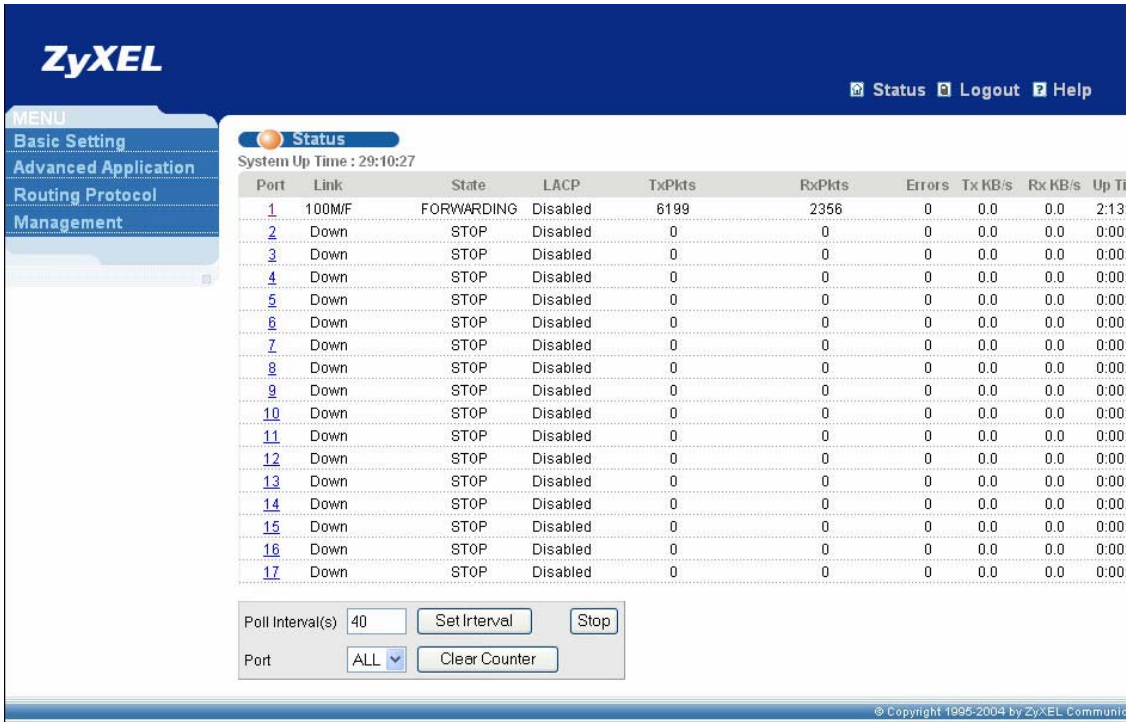
Configuring Switch A, E, F and H Using the Web Configurator

On switches A, E, F and H, create a VLAN (with VID 1) which contains all the port members. By default VLAN1 is already created for you. The setting required is to make sure that port 17 is a member of VLAN 1 and that egress tagging is enabled on the port.
*By default all the ports in VLAN 1 are untagged during Egress.

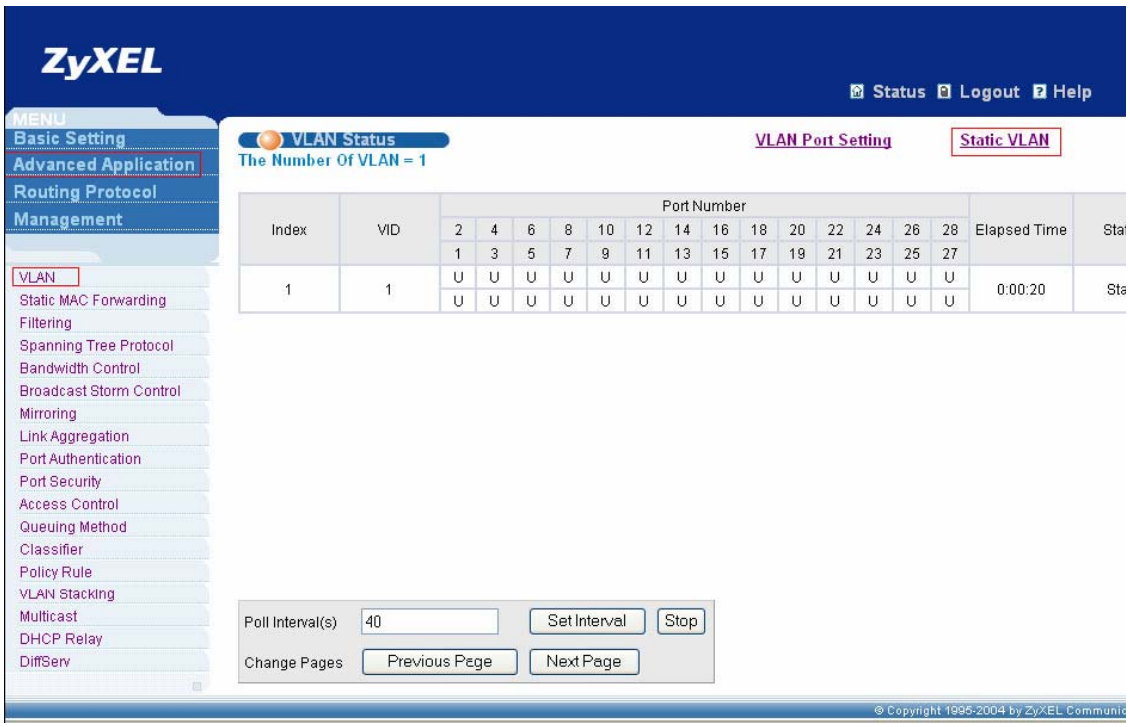
Configuring Switch B Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect your computer to the MGMT port on the switch.
2. By default, the IP address on the MGMT port is 192.168.0.1/24
3. Set your computer to use a static IP address in the same subnet (for example, 192.168.0.2/24).
4. Open a web browser (such as IE) and enter http://192.168.0.1 as the URL.
5. A login screen displays. Enter “admin” (the default) as the username and “1234” (the default) as the password.
6. After you have logged in successfully, the main screen displays as shown.

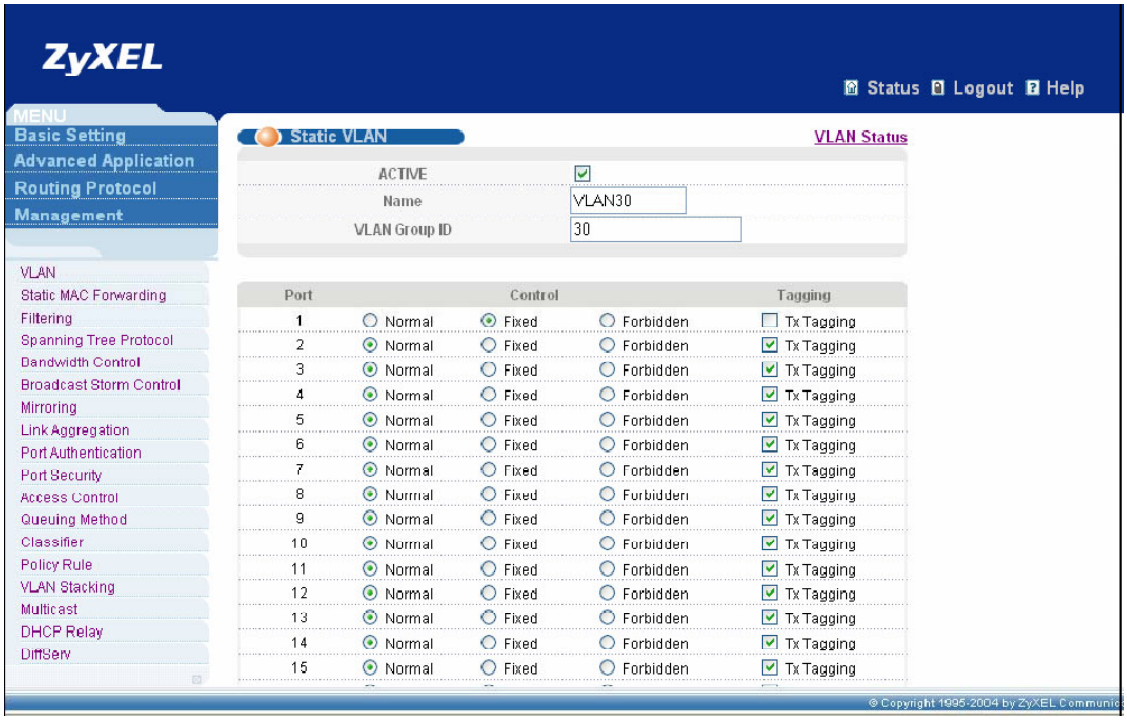
All contents copyright 2008 ZyXEL Communications Corporation.


ZyXEL
Status Logout Help
MENU
Basic Setting
Advanced Application
Routing Protocol
Management
Status
System Up Time : 29:10:27
Port Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Ti
1 100M/F FORWARDING Disabled 6199 2356 0 0.0 0.0 2:13
2 Down STOP Disabled 0 0 0 0.0 0.0 0:00
3 Down STOP Disabled 0 0 0 0.0 0.0 0:00
4 Down STOP Disabled 0 0 0 0.0 0.0 0:00
5 Down STOP Disabled 0 0 0 0.0 0.0 0:00
6 Down STOP Disabled 0 0 0 0.0 0.0 0:00
7 Down STOP Disabled 0 0 0 0.0 0.0 0:00
8 Down STOP Disabled 0 0 0 0.0 0.0 0:00
9 Down STOP Disabled 0 0 0 0.0 0.0 0:00
10 Down STOP Disabled 0 0 0 0.0 0.0 0:00
11 Down STOP Disabled 0 0 0 0.0 0.0 0:00
12 Down STOP Disabled 0 0 0 0.0 0.0 0:00
13 Down STOP Disabled 0 0 0 0.0 0.0 0:00
14 Down STOP Disabled 0 0 0 0.0 0.0 0:00
15 Down STOP Disabled 0 0 0 0.0 0.0 0:00
16 Down STOP Disabled 0 0 0 0.0 0.0 0:00
17 Down STOP Disabled 0 0 0 0.0 0.0 0:00
Poll Interval(s) 40 Set Irterval Stop
Port ALL Clear Counter
© Copyright 1995-2004 by ZyXEL Communic

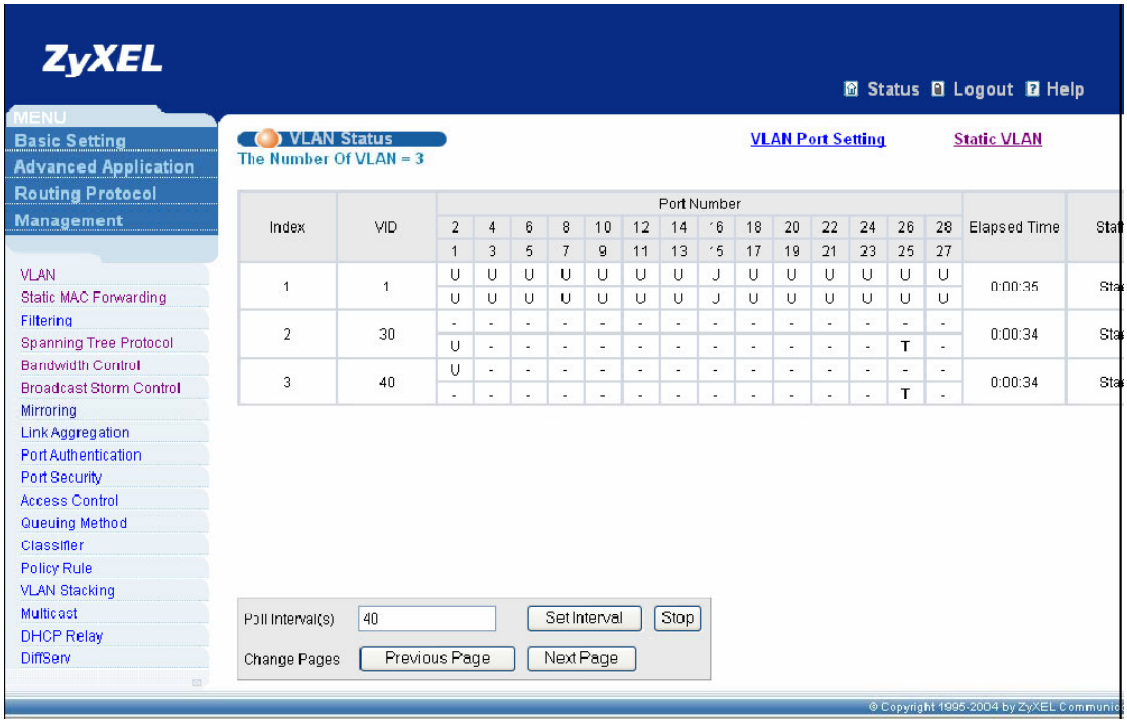
7. First, create VLAN groups for the ISP's network. For this example, VLAN 30 for company XX and VLAN 40 for company YY. Click **Advanced Application> Switch Advance> VLAN** and click the **Static VLAN** link.



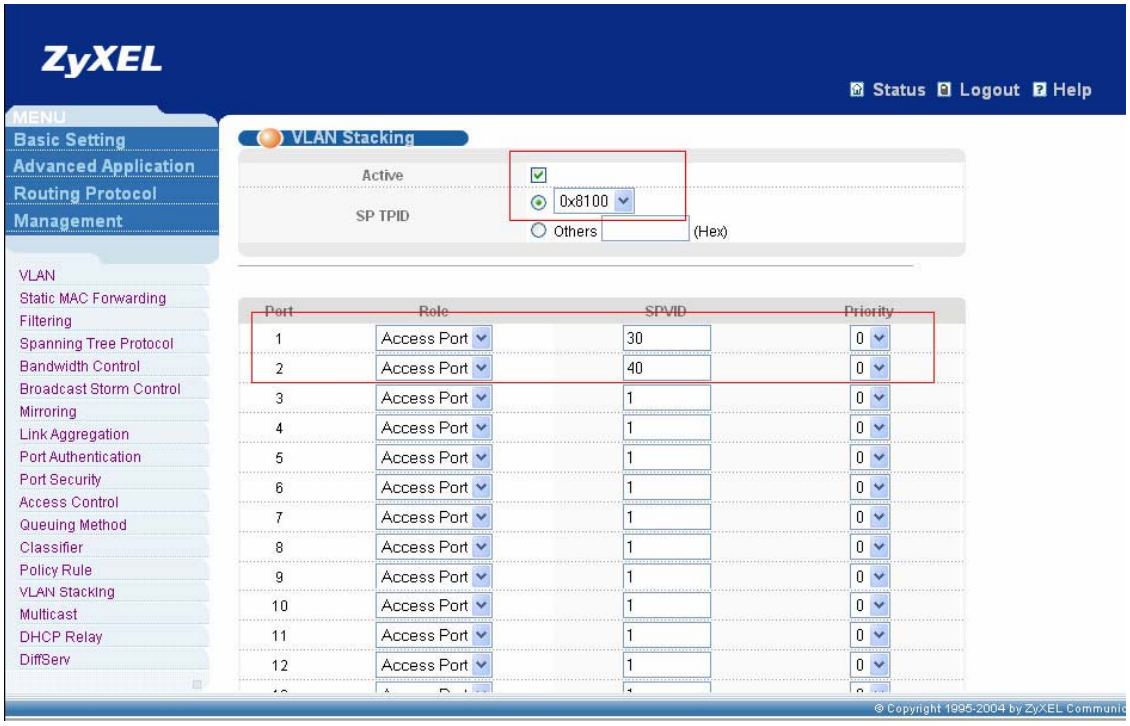
8. Create a VLAN with a VID of 30. Select **Fixed** and un-select **Tx Tagging** for port 1. For port 25, select both **Fixed** and **Tx Tagging**.



9. Create another VLAN with a VID of 40. Select **Fixed** and un-select **Tx Tagging** for port 2.
10. For port 12, select both **Fixed** and **Tx Tagging**. The **VLAN Status** screen should display as shown.



11. To configure VLAN Stacking, click **Advanced Application > VLAN Stacking** in the navigation panel to display the configuration screen.



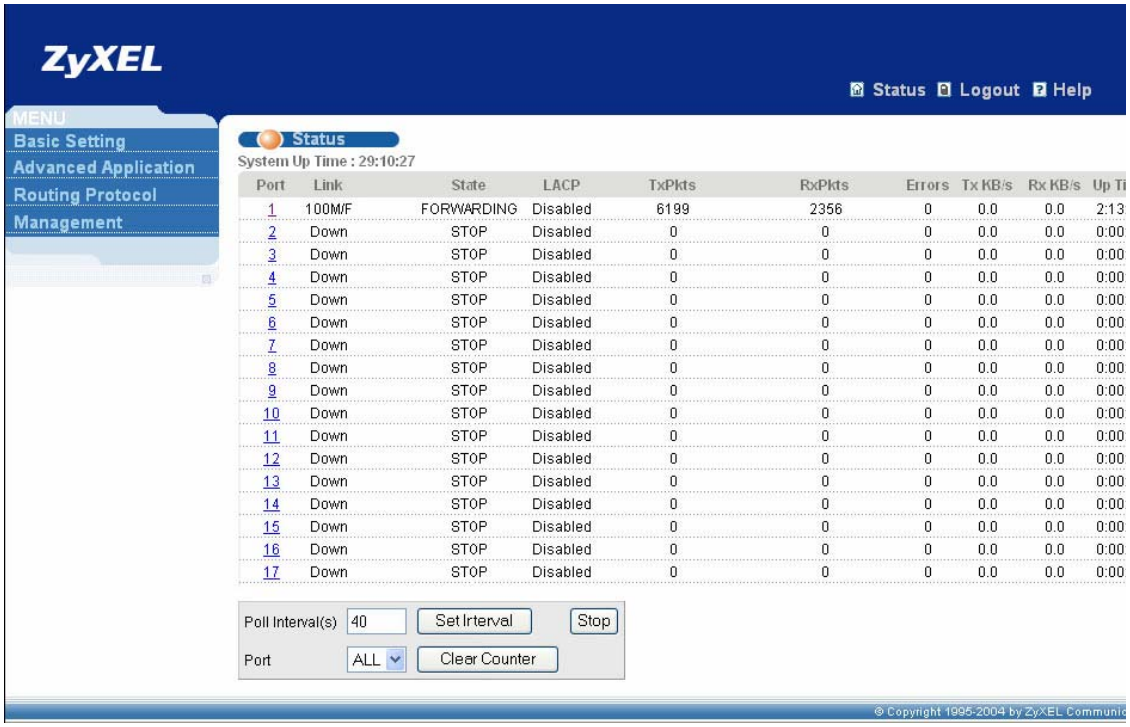
13. To enable VLAN stacking, select **Active**. Set ports 1 and 2 as the access port and enter the corresponding SPVIDs as shown in the figure above.

All contents copyright 2008 ZyXEL Communications Corporation.

14. Set port 25 as the “Tunnel Port” and leave the SPVID field to the default setting.
15. You have finished setting Switch B for VLAN stacking for this network example.

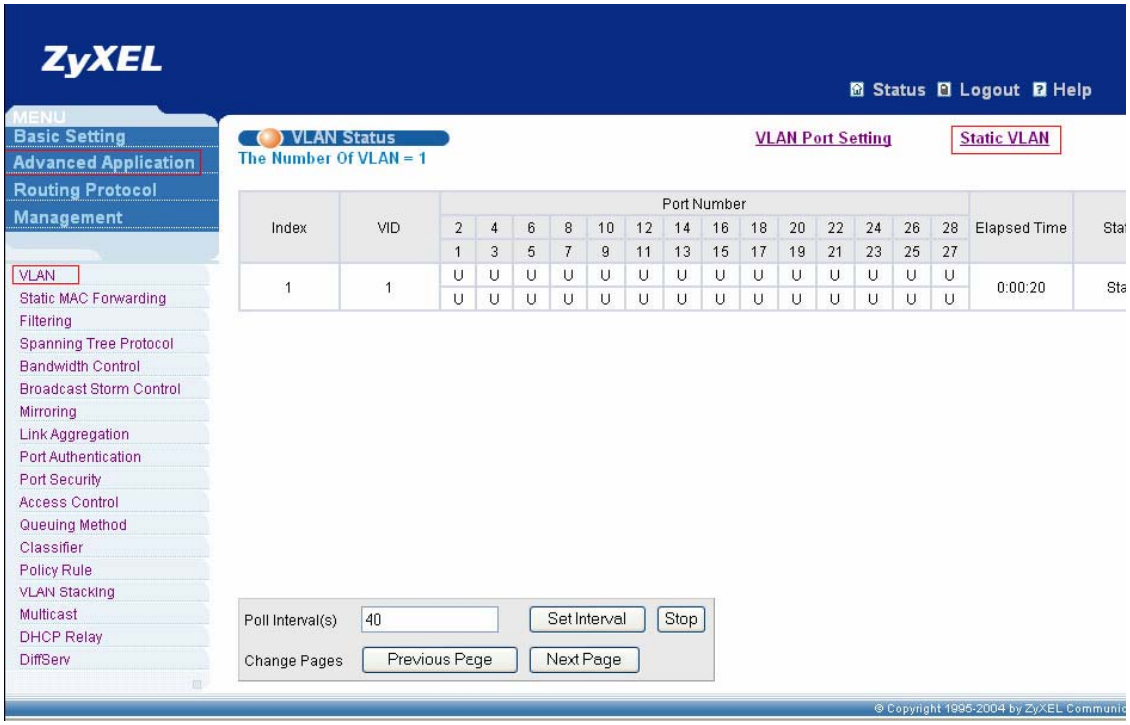
Configuring Switch C Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect your computer to the MGMT port on the switch.
2. By default, the IP address on the MGMT port is 192.168.0.1/24
3. Set your computer to use a static IP address in the same subnet (for example, 192.168.0.2/24).
4. Open a web browser (such as IE) and enter http://192.168.0.1 as the URL.
5. A login screen displays. Enter “admin” (the default) as the username and “1234” (the default) as the password.
6. After you have logged in successfully, the main screen displays as shown.

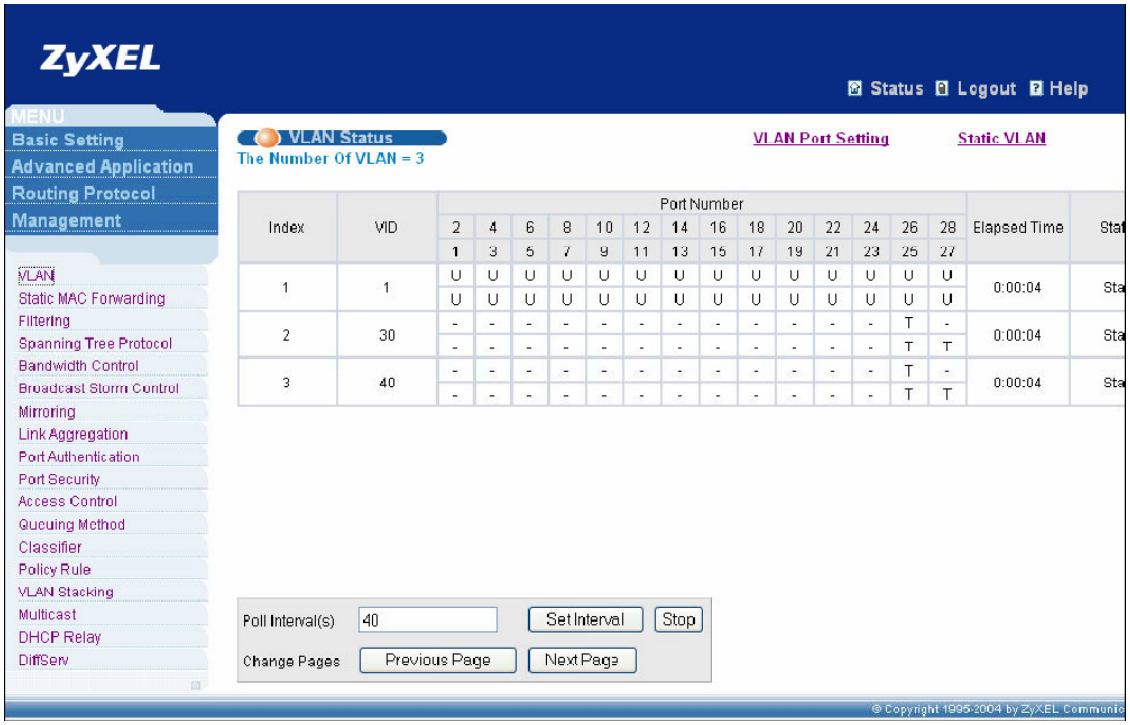

ZyXEL
Status Logout Help
MENU
Basic Setting
Advanced Application
Routing Protocol
Management
Status
System Up Time : 29:10:27
Port Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Ti
1 100M/F FORWARDING Disabled 6199 2356 0 0.0 0.0 2:13
2 Down STOP Disabled 0 0 0 0.0 0.0 0:00
3 Down STOP Disabled 0 0 0 0.0 0.0 0:00
4 Down STOP Disabled 0 0 0 0.0 0.0 0:00
5 Down STOP Disabled 0 0 0 0.0 0.0 0:00
6 Down STOP Disabled 0 0 0 0.0 0.0 0:00
7 Down STOP Disabled 0 0 0 0.0 0.0 0:00
8 Down STOP Disabled 0 0 0 0.0 0.0 0:00
9 Down STOP Disabled 0 0 0 0.0 0.0 0:00
10 Down STOP Disabled 0 0 0 0.0 0.0 0:00
11 Down STOP Disabled 0 0 0 0.0 0.0 0:00
12 Down STOP Disabled 0 0 0 0.0 0.0 0:00
13 Down STOP Disabled 0 0 0 0.0 0.0 0:00
14 Down STOP Disabled 0 0 0 0.0 0.0 0:00
15 Down STOP Disabled 0 0 0 0.0 0.0 0:00
16 Down STOP Disabled 0 0 0 0.0 0.0 0:00
17 Down STOP Disabled 0 0 0 0.0 0.0 0:00
Poll Interval(s) 40 Set Interval Stop
Port ALL Clear Counter
© Copyright 1995-2004 by ZyXEL Communic

7. First, create VLAN groups for the ISP’s network. For this example, VLAN 30 for company XX and VLAN 40 for company YY. Click **Advanced Application> Switch Advance> VLAN** and click the **Static VLAN** link.

All contents copyright 2008 ZyXEL Communications Corporation.

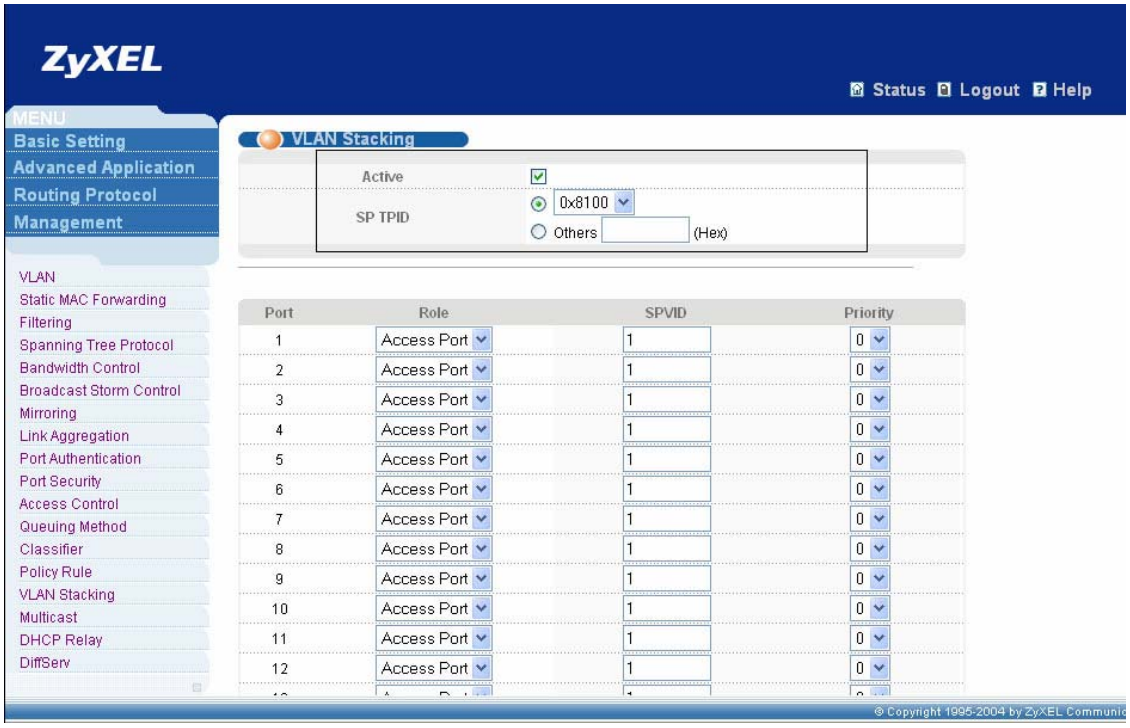


Follow the steps in the previous section to configure VLANs 30 and 40 of which ports 9, 10 and 11 are members. After the configuration, the **VLAN Status** screen should look similar to the figure as shown.

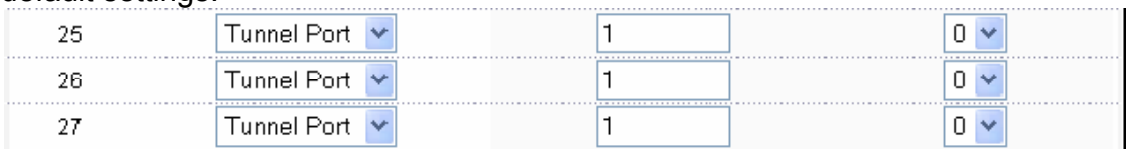


11. To configure VLAN Stacking, click **Advanced Application > VLAN Stacking**

in the navigation panel to display the configuration screen.



Set ports 25, 26 and 27 as the “Tunnel Ports” and leave the SPVID fields to the default settings.

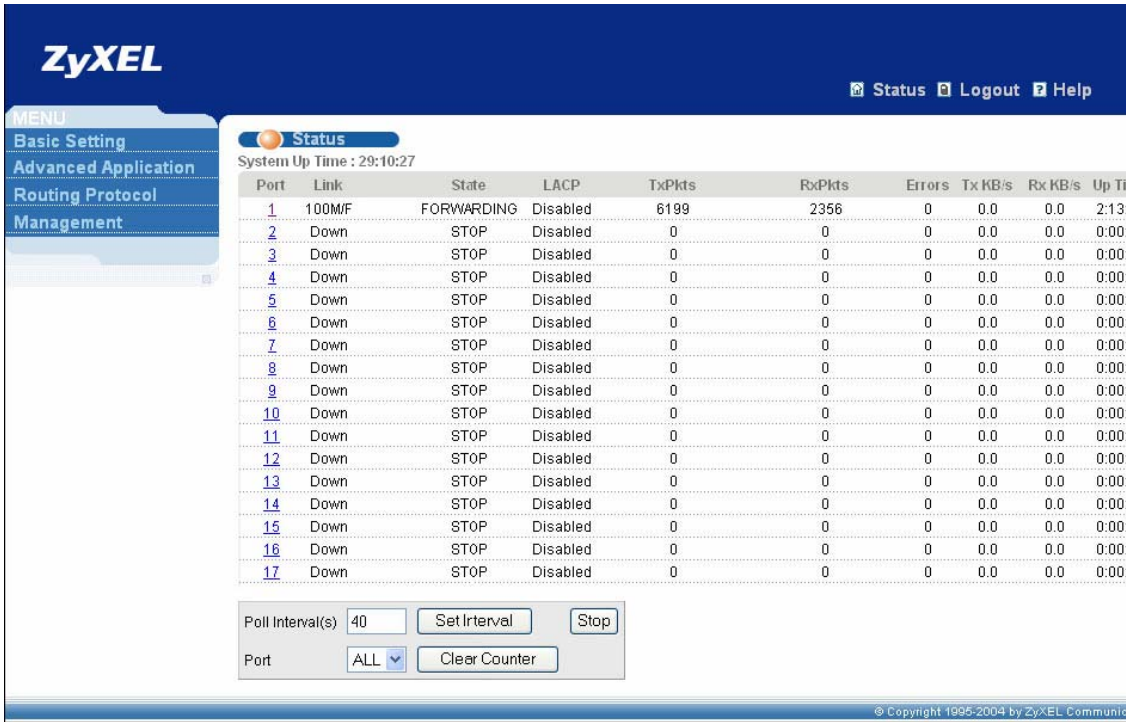


9. You have finished setting Switch C for VLAN stacking for this network example.

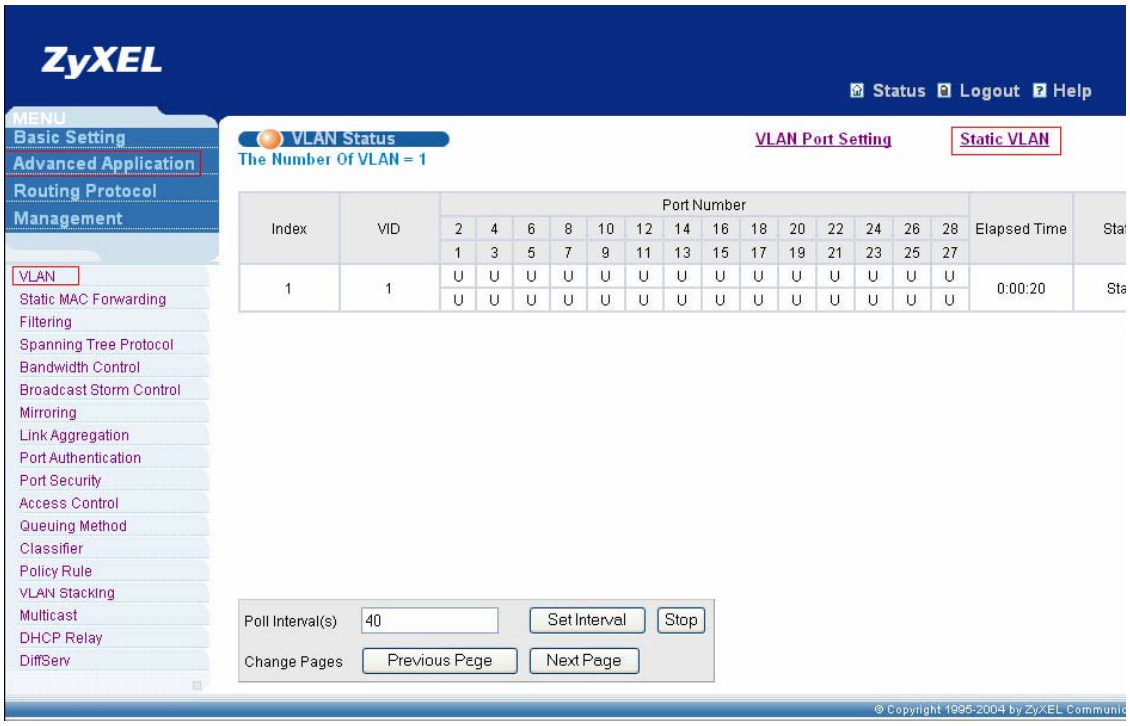
Configuring Switch D Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect your computer to the MGMT port on the switch.
2. By default, the IP address on the MGMT port is 192.168.0.1/24
3. Set your computer to use a static IP address in the same subnet (for example, 192.168.0.2/24).
4. Open a web browser (such as IE) and enter http://192.168.0.1 as the URL.
5. A login screen displays. Enter “admin” (the default) as the username and “1234” (the default) as the password.
6. After you have logged in successfully, the main screen displays as shown.

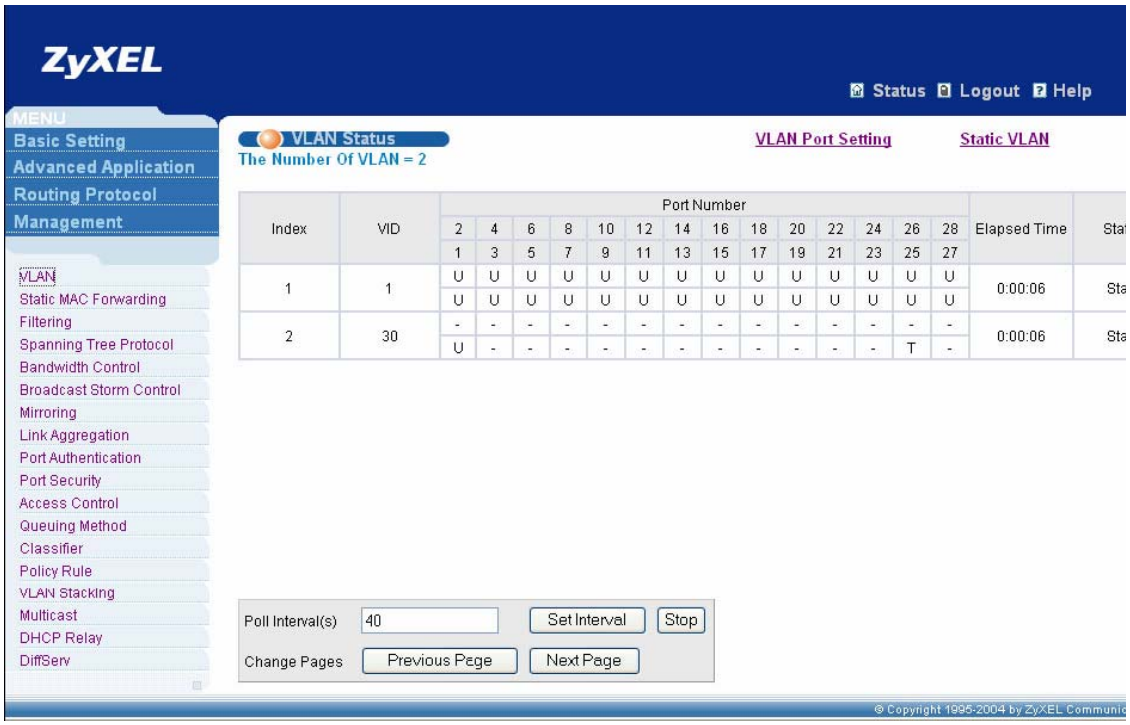
All contents copyright 2008 ZyXEL Communications Corporation.


ZyXEL
Status Logout Help
MENU
Basic Setting
Advanced Application
Routing Protocol
Management
Status
System Up Time : 29:10:27
Port Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Ti
1 100M/F FORWARDING Disabled 6199 2356 0 0.0 0.0 2:13
2 Down STOP Disabled 0 0 0 0.0 0.0 0:00
3 Down STOP Disabled 0 0 0 0.0 0.0 0:00
4 Down STOP Disabled 0 0 0 0.0 0.0 0:00
5 Down STOP Disabled 0 0 0 0.0 0.0 0:00
6 Down STOP Disabled 0 0 0 0.0 0.0 0:00
7 Down STOP Disabled 0 0 0 0.0 0.0 0:00
8 Down STOP Disabled 0 0 0 0.0 0.0 0:00
9 Down STOP Disabled 0 0 0 0.0 0.0 0:00
10 Down STOP Disabled 0 0 0 0.0 0.0 0:00
11 Down STOP Disabled 0 0 0 0.0 0.0 0:00
12 Down STOP Disabled 0 0 0 0.0 0.0 0:00
13 Down STOP Disabled 0 0 0 0.0 0.0 0:00
14 Down STOP Disabled 0 0 0 0.0 0.0 0:00
15 Down STOP Disabled 0 0 0 0.0 0.0 0:00
16 Down STOP Disabled 0 0 0 0.0 0.0 0:00
17 Down STOP Disabled 0 0 0 0.0 0.0 0:00
Poll Interval(s) 40 Set Interval Stop
Port ALL Clear Counter
© Copyright 1995-2004 by ZyXEL Communic

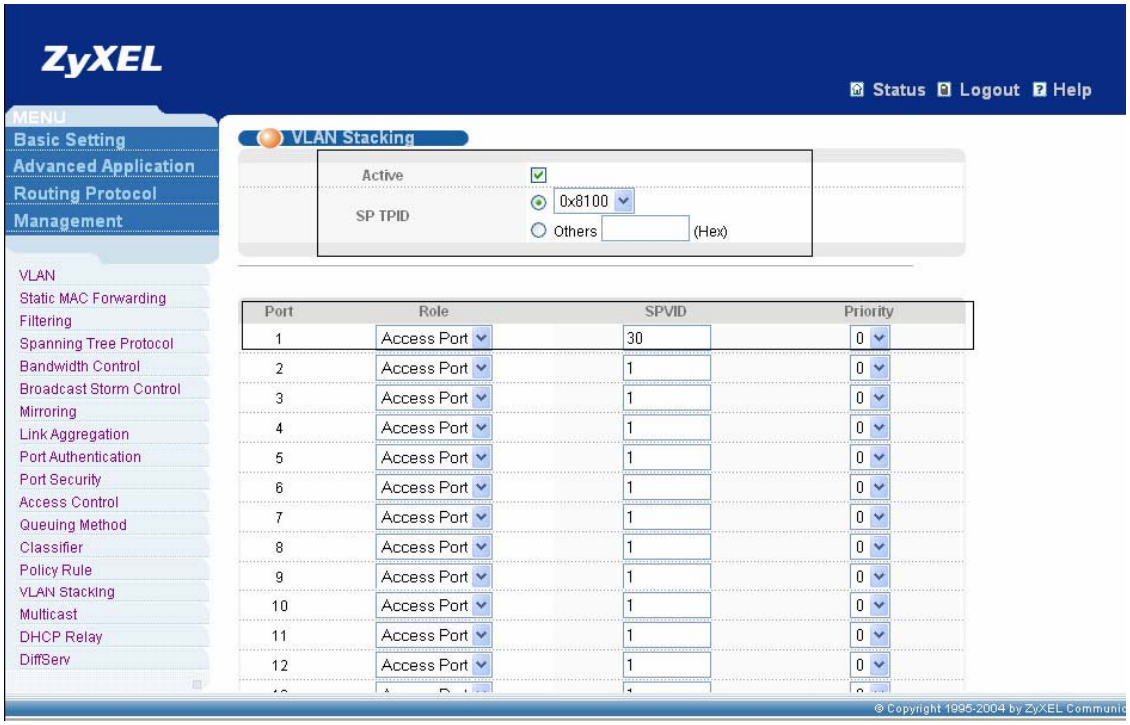
7. First, create VLAN groups for the ISP's network. For this example, VLAN 30 for company XX and VLAN 40 for company YY. Click **Advanced Application> Switch Advance> VLAN** and click the **Static VLAN** link.



Follow the steps in the previous section to configure VLAN 30 of which ports 1 and 12 are members. Since port 1 is an Access Port, un-select the **Tx Tagging** field. After the configuration, the **VLAN Status** screen should look similar to the figure as shown.



8. To configure VLAN Stacking, click **Advanced Application > VLAN Stacking** in the navigation panel to display the configuration screen.



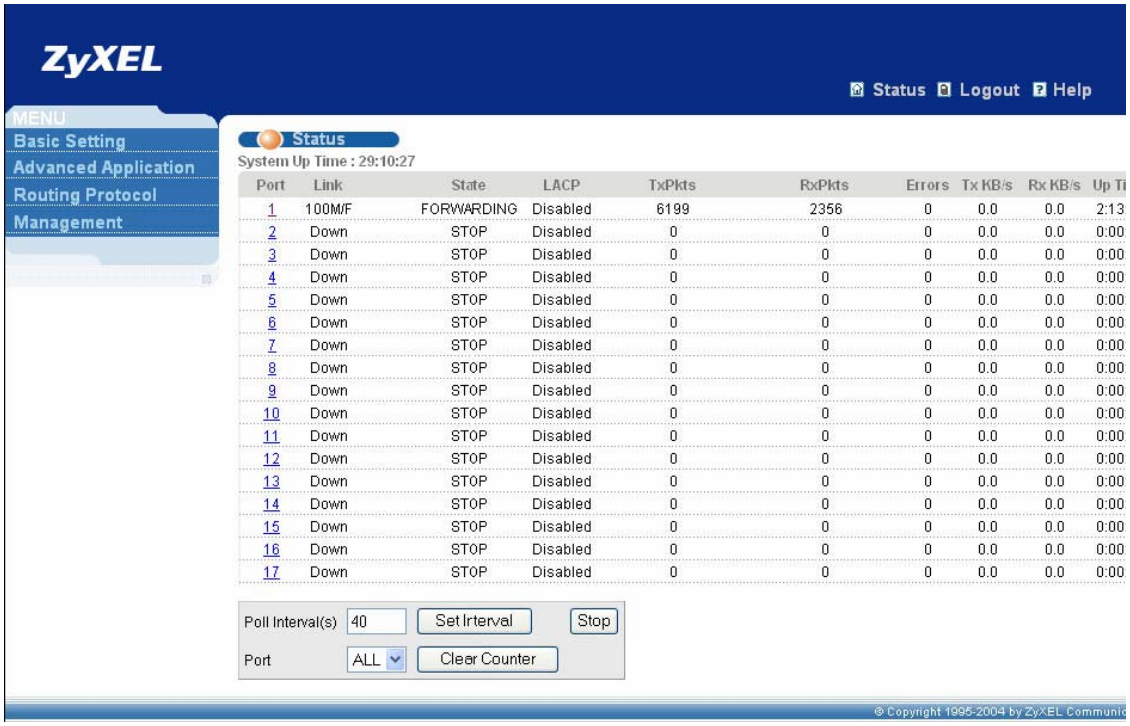
To enable VLAN stacking, select **Active**. Set port 25 as the tunnel port and leave the SPVID field to the default settings.

9. You have finished setting Switch D for VLAN stacking for this network example.

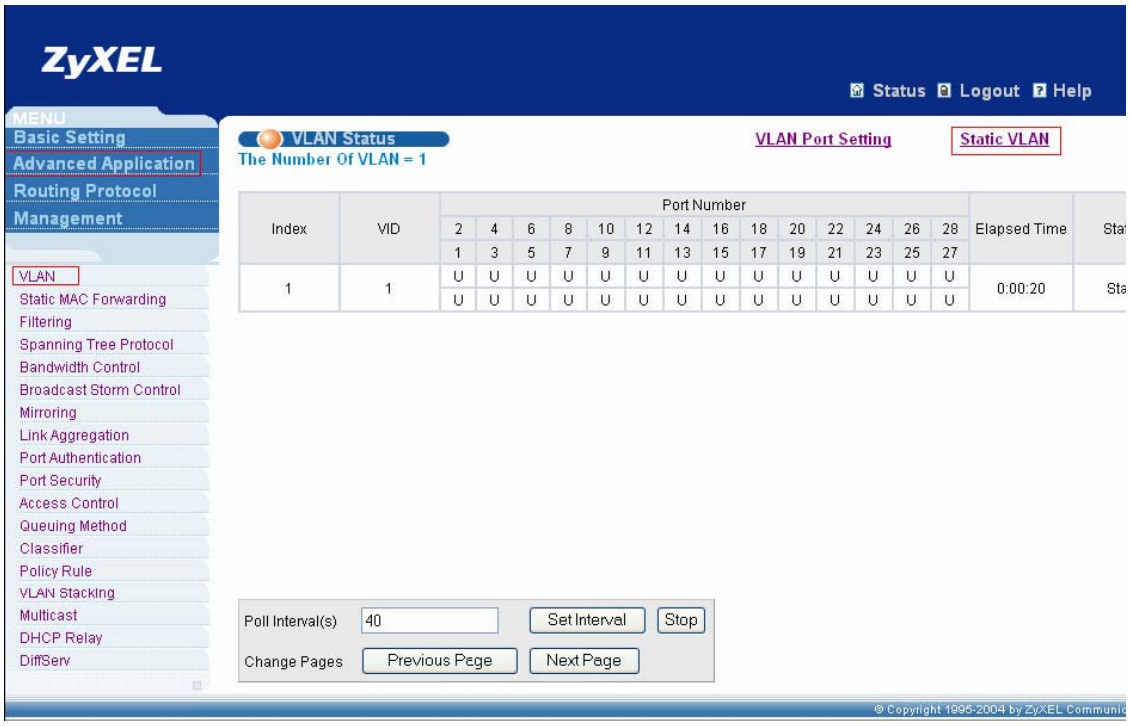
Configuring Switch G Using the Web Configurator

1. Use an RJ-45 Ethernet cable to connect your computer to the MGMT port on the switch.
2. By default, the IP address on the MGMT port is 192.168.0.1/24
3. Set your computer to use a static IP address in the same subnet (for example, 192.168.0.2/24).
4. Open a web browser (such as IE) and enter http://192.168.0.1 as the URL.
5. A login screen displays. Enter “admin” (the default) as the username and “1234” (the default) as the password.
6. After you have logged in successfully, the main screen displays as shown.

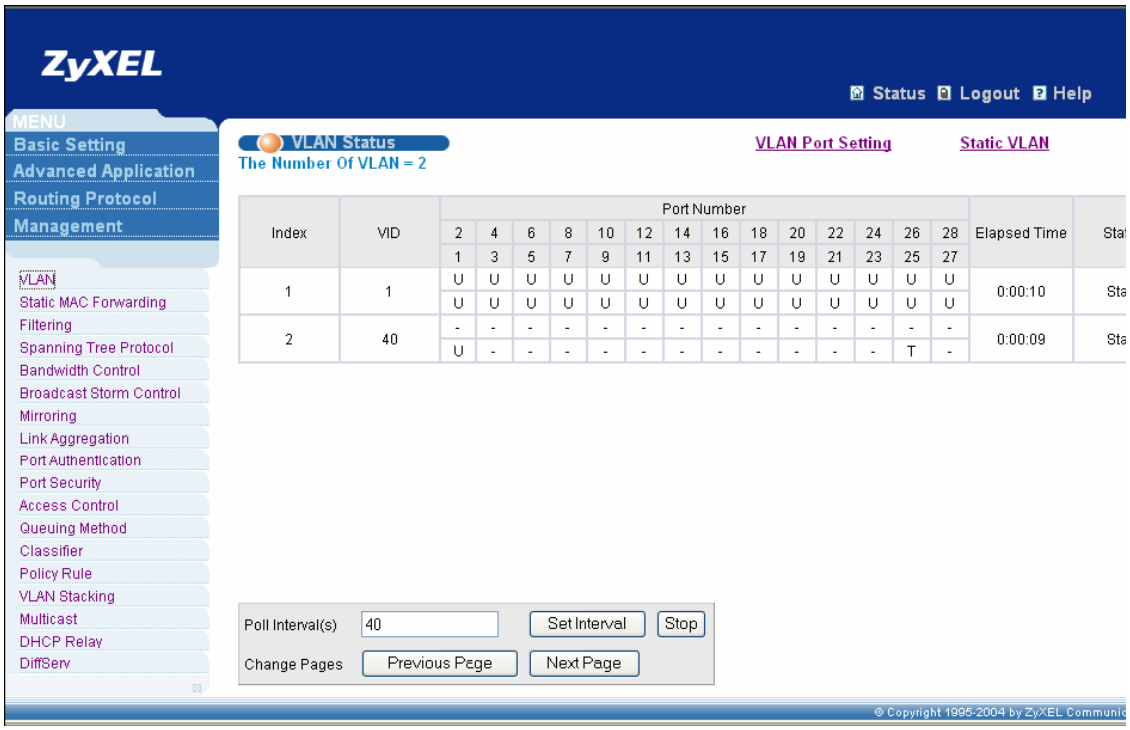
All contents copyright 2008 ZyXEL Communications Corporation.


ZyXEL
Status Logout Help
MENU
Basic Setting
Advanced Application
Routing Protocol
Management
Status
System Up Time : 29:10:27
Port Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Ti
1 100M/F FORWARDING Disabled 6199 2356 0 0.0 0.0 2:13
2 Down STOP Disabled 0 0 0 0.0 0.0 0:00
3 Down STOP Disabled 0 0 0 0.0 0.0 0:00
4 Down STOP Disabled 0 0 0 0.0 0.0 0:00
5 Down STOP Disabled 0 0 0 0.0 0.0 0:00
6 Down STOP Disabled 0 0 0 0.0 0.0 0:00
7 Down STOP Disabled 0 0 0 0.0 0.0 0:00
8 Down STOP Disabled 0 0 0 0.0 0.0 0:00
9 Down STOP Disabled 0 0 0 0.0 0.0 0:00
10 Down STOP Disabled 0 0 0 0.0 0.0 0:00
11 Down STOP Disabled 0 0 0 0.0 0.0 0:00
12 Down STOP Disabled 0 0 0 0.0 0.0 0:00
13 Down STOP Disabled 0 0 0 0.0 0.0 0:00
14 Down STOP Disabled 0 0 0 0.0 0.0 0:00
15 Down STOP Disabled 0 0 0 0.0 0.0 0:00
16 Down STOP Disabled 0 0 0 0.0 0.0 0:00
17 Down STOP Disabled 0 0 0 0.0 0.0 0:00
Poll Interval(s) 40 Set Interval Stop
Port ALL Clear Counter
© Copyright 1995-2004 by ZyXEL Communic

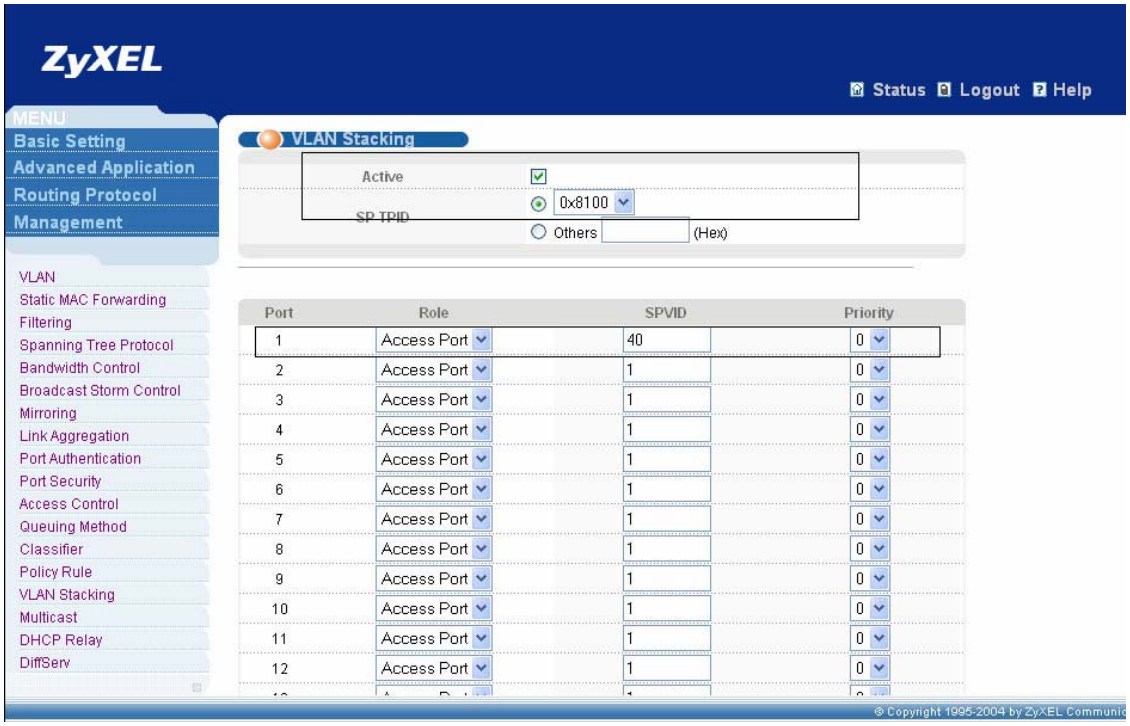
7. First, create VLAN groups for the ISP's network. For this example, VLAN 30 for company XX and VLAN 40 for company YY. Click **Advanced Application> Switch Advance> VLAN** and click the **Static VLAN** link.



Follow the steps in the previous section to configure VLAN 40 of which ports 1 and 12 are members. Since port 12 is a TunnelPort, select the **Tx Tagging** field. For the Access Port (port 1), un-select the **Tx Tagging** field. After the configuration, the **VLAN Status** screen should look similar to the figure as shown.



8. To configure VLAN Stacking, click **Advanced Application > VLAN Stacking** in the navigation panel to display the configuration screen.

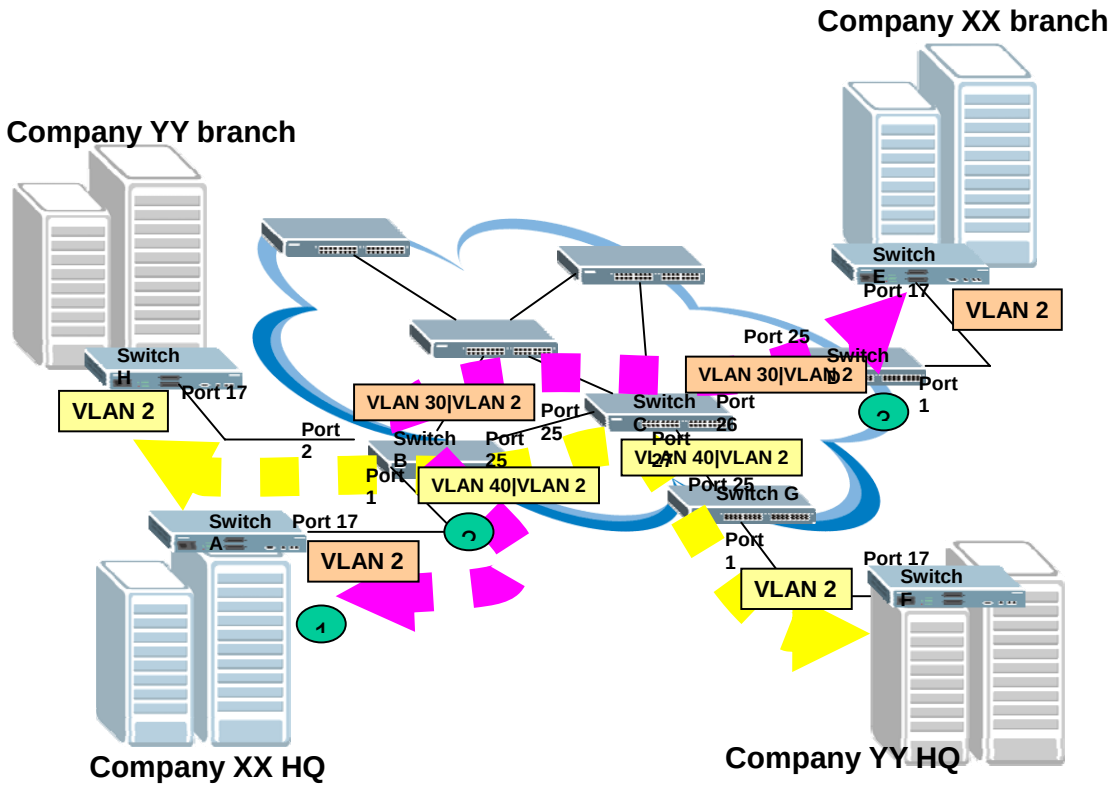


To enable VLAN stacking, select **Active**. Set port 25 as the tunnel port and leave the SPVID field to the default settings.

9. You have finished setting Switch G for VLAN stacking for this network example.

All contents copyright 2008 ZyXEL Communications Corporation.

Network Scenario



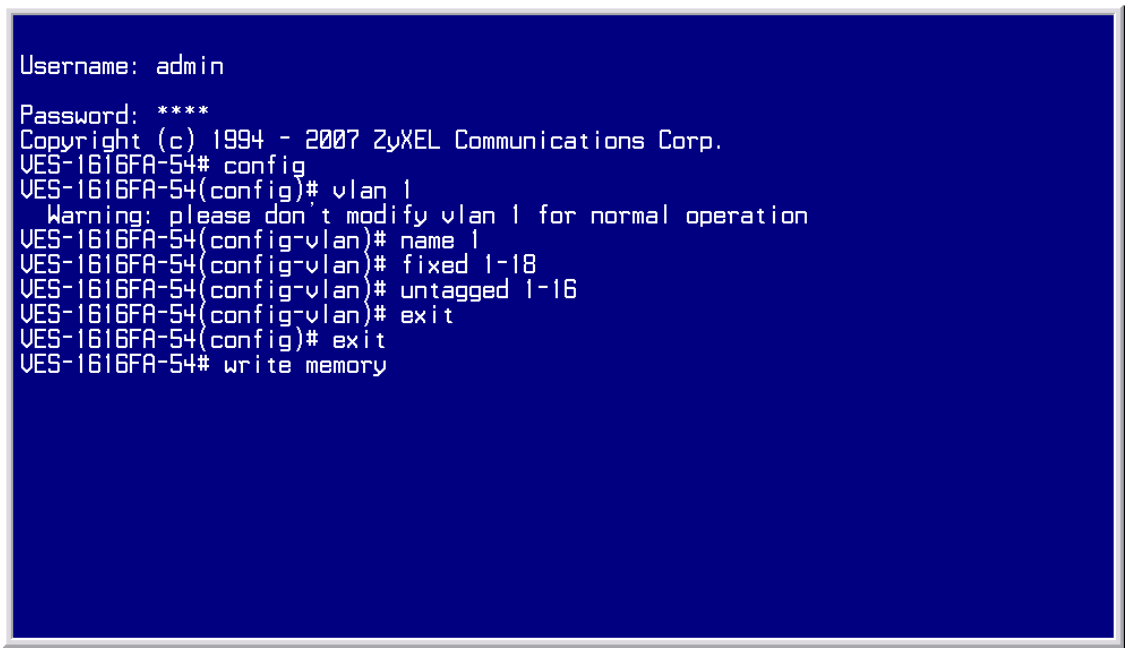
Configuring Switches A, E, F and H Using the CLI

On switches A, E, F and H, create a VLAN (with VID 1) which contains all the port members. By default VLAN1 is already created for you. The setting required is to make sure that port 17 is a member of VLAN 1 and that egress tagging is enabled on the port.
*By default all the ports in VLAN 1 are untagged during Egress.

1. On switches A, E, F and H, create a VLAN (with VID 1) which contains all the port members. By default VLAN1 is already created for you. The setting required is to make sure that port 17 is a member of VLAN 1 and that egress tagging is enabled on the port.
*By default all the ports in VLAN 1 are untagged during Egress.
2. Connect your computer to the console port on the switch.
3. Open a Terminal program (for example Hyper Terminal in Windows)
4. Configure the console port settings as shown next.
Bps: 9600

All contents copyright 2008 ZyXEL Communications Corporation.

Data bits: 8
Parity: None
Stop bits: 1
Flow control: None:
5. After you are connected successfully, the login prompt displays. Enter the administrator login username (“admin”) and password (“1234” is the default).
6. Enter “config” to go into the configuration mode.
7. Enter the commands as shown in the screen to configure VLAN 1 on switches A, E, F and H for this network scenario. (Port 17 will be tagged during Egress)



8. After entering the commands, use the “write memory” command in the enable mode to save your configuration.

Configuring Switch B Using the CLI

1. Connect your computer to the console port on the switch.
2. Open a Terminal program (for example Hyper Terminal in Windows)
3. Configure the console port settings as shown next.
Bps: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None:
4. After you are connected successfully, the login prompt displays. Enter the administrator login username (“admin”) and password (“1234” is the default).
5. Enter “config” to go into the configuration mode.
6. Enter the commands as shown in the screen to configure VLAN Stacking on

All contents copyright 2008 ZyXEL Communications Corporation.

switch B for this network scenario.

```
vlan 30
name VLAN30
normal 2-24,26-28
fixed 1,25
forbidden ""
untagged 1
exit

vlan 40
name VLAN40
normal 1,3-24,26-28
fixed 2,25
forbidden ""
untagged 2
exit

interface port-channel 1
vlan-stacking SPVID 30
exit

interface port-channel 2
vlan-stacking SPVID 40
exit

interface port-channel 25
vlan-stacking role tunnel
exit

vlan-stacking
```

7. After entering the commands, use the “write memory” command in the enable mode to save your configuration.

Configuring Switch C via CLI

1. Connect your computer to the console port on the switch.
2. Open a Terminal program (for example Hyper Terminal in Windows)
3. Configure the console port settings as shown next
Bps: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None:
4. After you are connected successfully, the login prompt displays. Enter the administrator login username (“admin”) and password (“1234” is the default).
5. Enter “config” to go into the configuration mode.
6. Enter the commands as shown in the screen to configure VLAN Stacking on switch C for this network scenario.

All contents copyright 2008 ZyXEL Communications Corporation.

```
vlan 30
name VLAN30
normal 1-24,28
fixed 25-27
forbidden ""
untagged ""
exit

vlan 40
name VLAN40
normal 1-24,28
fixed 25-27
forbidden ""
untagged ""
exit

interface port-channel 25
vlan-stacking role tunnel
exit

interface port-channel 26
vlan-stacking role tunnel
exit

interface port-channel 27
vlan-stacking role tunnel
exit

vlan-stacking
```

7. After entering the commands, use the “write memory” command in the enable mode to save your configuration.

Configuring Switch D Using the CLI

1. Connect your computer to the console port on the switch.
2. Open a Terminal program (for example Hyper Terminal in Windows)
3. Configure the console port settings as shown next
Bps: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None:
4. After you are connected successfully, the login prompt displays. Enter the administrator login username (“admin”) and password (“1234” is the default).
5. Enter “config” to go into the configuration mode.
6. Enter the commands as shown in the screen to configure VLAN Stacking on switch D for this network scenario.

All contents copyright 2008 ZyXEL Communications Corporation.

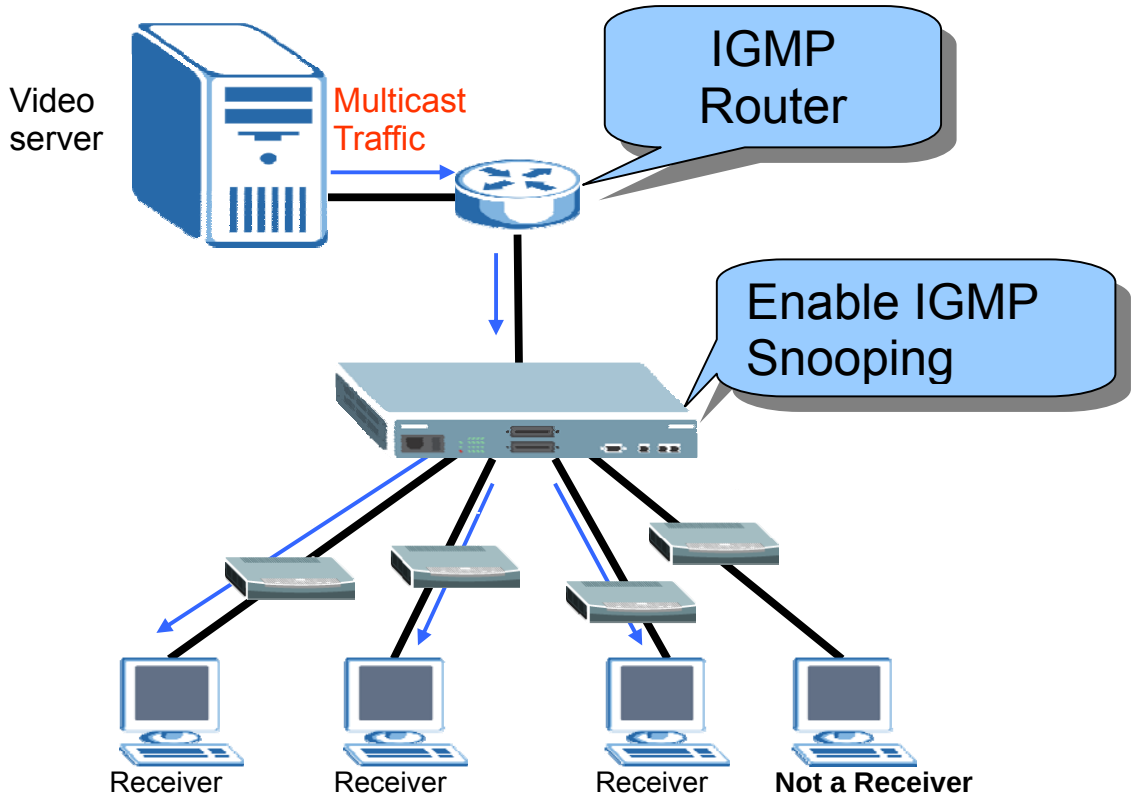
```
vlan 40
name VLAN40
normal 2-24,26-28
fixed 1,25
forbidden ""
untagged 1
exit

interface port-channel 1
vlan-stacking SPVID 40
exit

interface port-channel 25
vlan-stacking role tunnel
exit

vlan-stacking
```

6. After entering the commands, use the “write memory” command in the enable mode to save your configuration.

All contents copyright 2008 ZyXEL Communications Corporation.

IP Multicasting

Configuring IGMP snooping in your switch



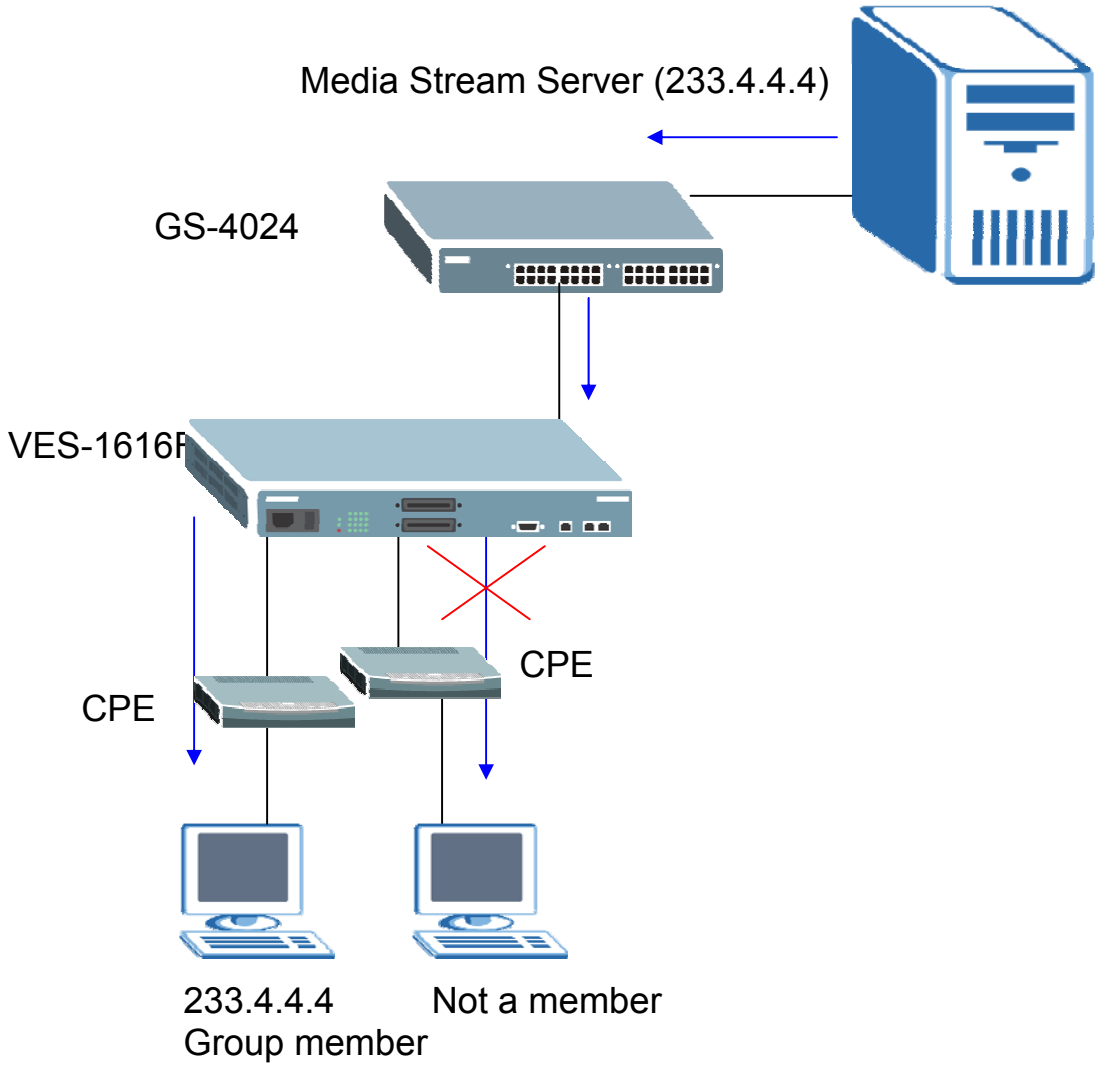
IGMP snooping is designed for scenarios with multicast traffic.
It operates on the underlying IGMP mechanism where a layer two switch passively listens to the IGMP Query, Report and Leave (IGMP version 2) packets transmitted between the IGMP router and clients and collects passing IGMP messages. After that, the switch records the message's group registration information, and configures the multicasting information accordingly. If the multicast group information is unknown (not recorded on the switch), the switch discards that multicast traffic. Only the registered clients that join the group will receive multicast stream from the IGMP router. Thus this significantly reduces the multicast traffic forwarded down to the clients.
Another advantage of IGMP snooping is to allow the intermediate switch to learn

All contents copyright 2008 ZyXEL Communications Corporation.

multicast group information without manually configuring switches.

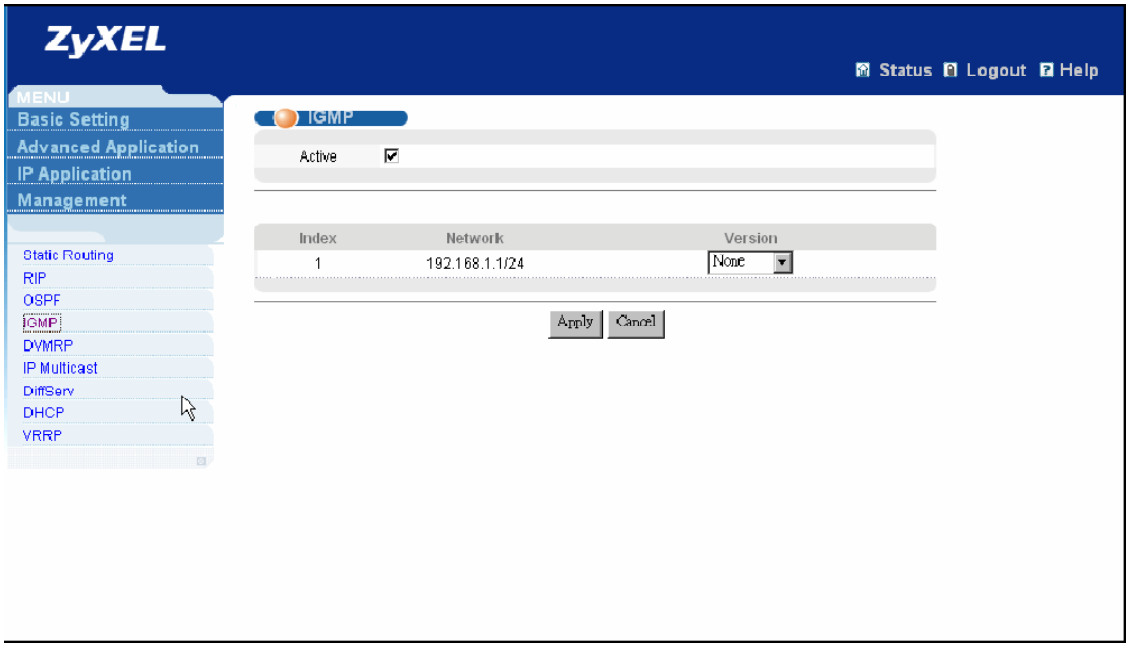
Configuration of IGMP snooping by web

In this example, we enable the IGMP function on the GS-4024 (an IGMP router) to connect to a multimedia server. Also, we enable IGMP snooping function on the VES-1616F-3X the multimedia clients are connect to.

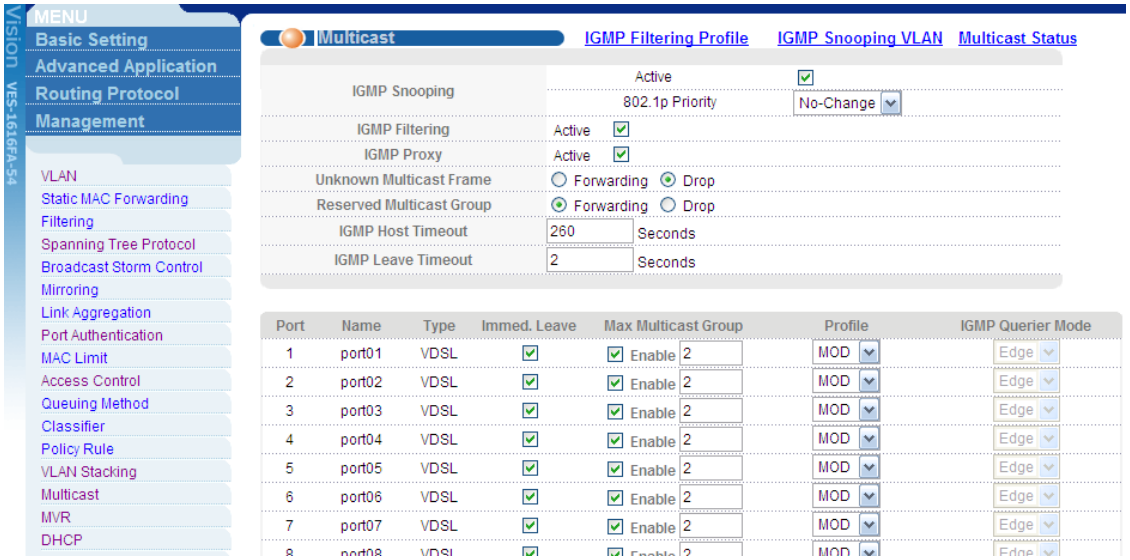


1. In GS-4024, click the **IP Application**, select **IGMP** where, IGMP function can be enabled and we can select either IGMP-v1 or IGMP-v2.

All contents copyright 2008 ZyXEL Communications Corporation.



2. In the VDSL Switch, click **Advanced Application > Multicast > Multicast Setting** and then **IGMP Snooping** where we can enable IGMP snooping function with WEB-GUI.



Configuration of IGMP and IGMP snooping by CLI

1. Enable IGMP function in GS-4024
In the configure mode
GS-4024(config)# **router igmp**
2. Enable IGMP snooping in VDSL switch
In the configure mode of CLI,

All contents copyright 2008 ZyXEL Communications Corporation.

VES-1616FA-54(config)# **igmp-snooping**
3. Display the IGMP Status
In the exec mode of CLI
VES-1616FA-54# **show multicast**
4. Display the IGMP snooping Status
In the exec mode of CLI
VES-1616FA-54# **show igmp-snooping**

Note: One thing needs to be mentioned is that in the IGMP router, we do not need to enable IGMP snooping function.

Overview of MVR

MVR refers to Multicast VLAN Registration that enables a media server to transmit multicast stream in a single multicast VLAN while clients receiving multicast VLAN stream can reside in different VLANs. Clients in different VLANs intending to join or leave the multicast group simply send the IGMP Join/leave message to a receiver port. The receiver port belonging to one of the multicast groups can receive multicast stream from media server. In the Figure 1, without support of MVR, the Multicast stream from the media server and the subscriber must reside in the same VLAN. For each VLAN, A media server is required to transmit multicast stream once and totally, media server transmits 6 times. In the Figure 2, on the contrary, with MVR, a media server is required to transmit multicast traffic to clients in different VLANs at once.

All contents copyright 2008 ZyXEL Communications Corporation.

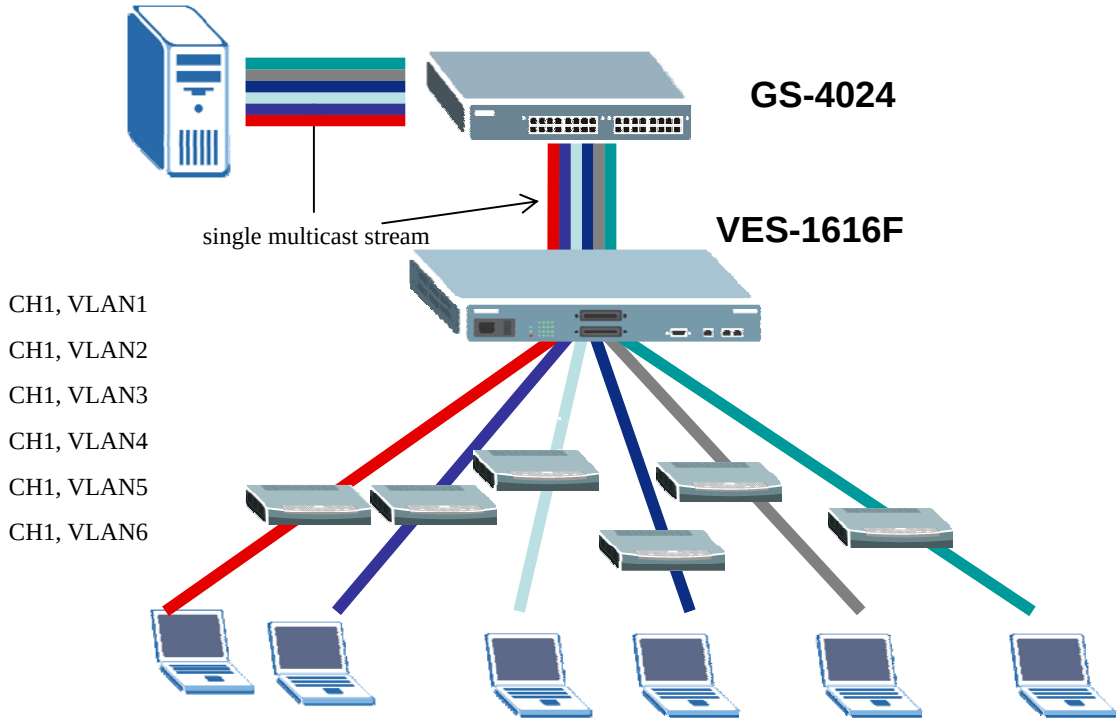


Figure 1

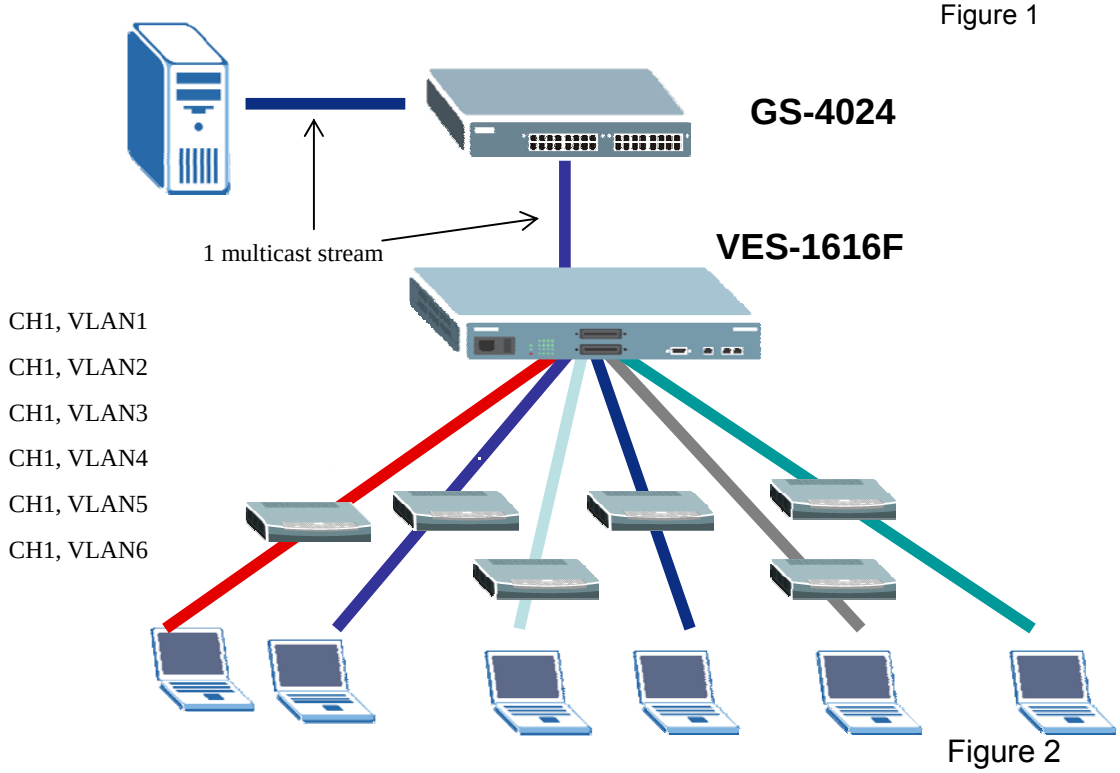


Figure 2

MVR Mode

- **Dynamic Mode**

If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will be forwarded to a multicast router through its source

All contents copyright 2008 ZyXEL Communications Corporation.

port. Multicast router knows which multicast groups exist on which interface dynamically.

- **Compatible mode**

If we select the dynamic mode in MVR setting, IGMP report message transmitted from the receiver port will not be transmitted to a multicast router. Multicast router must be statically configured.

Operation Mode

- **Join Operation**

A subscriber sends an IGMP report message to the switch to join the appropriate multicast. It tests whether the IGMP report matches the switch configured multicast MAC address. If matches, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the MVLAN

- **Leave Operation**

Subscriber sends an IGMP leave message to the switch to leave the multicast. The switch CPU sends an IGMP group-specific query through the receiver port VLAN. If there is another subscriber in the VLAN, subscriber must respond within the max response time. If there is no subscriber, the switch eliminates this receiver port.

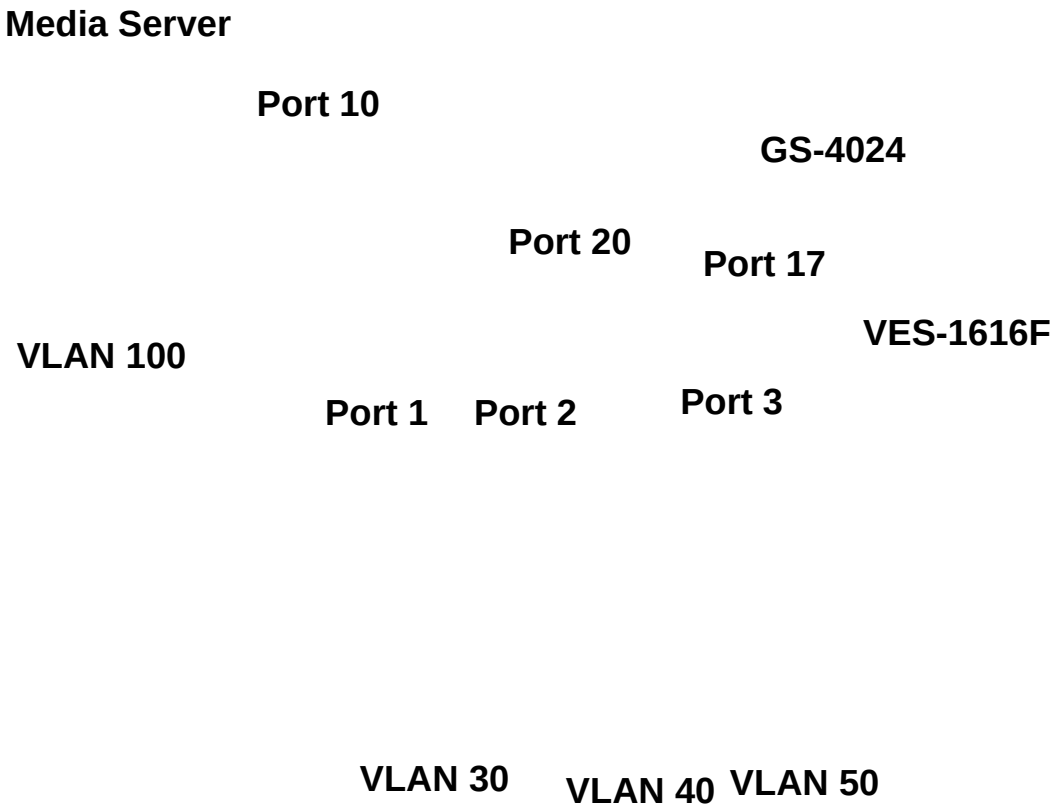
- **Immediate Leave Operation**

Subscriber sends an IGMP leave message to the switch to leave the multicast. Subscribers do not need to wait for the switch CPU to send an IGMP group-specific query through the receiver port VLAN. The switch will immediately eliminate this receiver port.

Scenario of MVR

In the following section, we will provide an example to illustrate how to configure MVR. In this scenario, the main job of media server is to transmit the media stream via port 10 to GS-4024. The multicast traffic flowing into the GS-4024 will be tagged with PVID=100. In the VES-1616F-3X, we enable the MVR function to allocate the multicast traffic from GS-4024 to separate VLAN hosts.

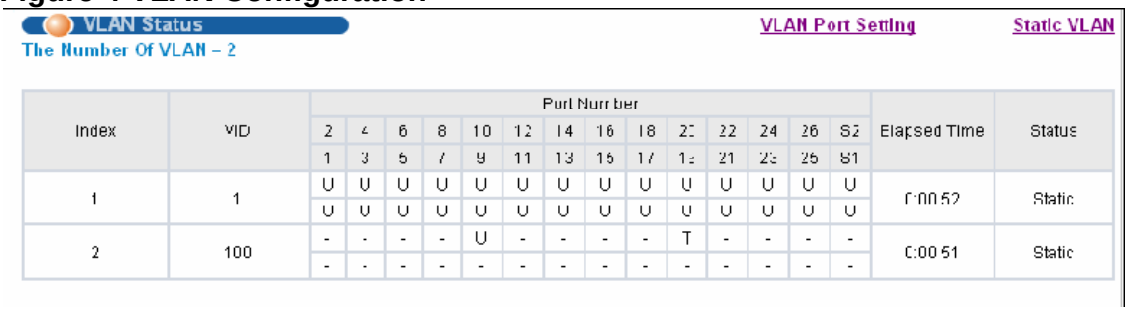
All contents copyright 2008 ZyXEL Communications Corporation.



Configuration via Web

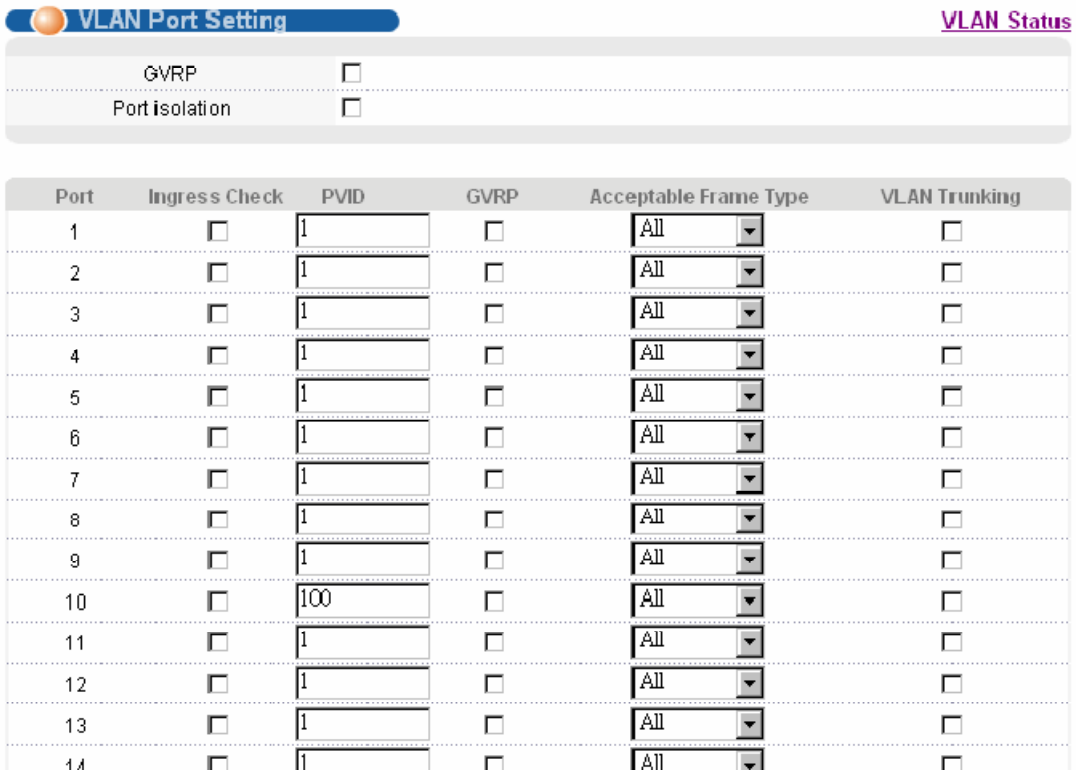
1. We need to create a VLAN for multicast traffic in GS-4024. In **GS-4024**, click the **Advanced Application** and then select the **VLAN.** In the VLAN Configuration, create a new VLAN 100.

Figure 4 VLAN Configuration

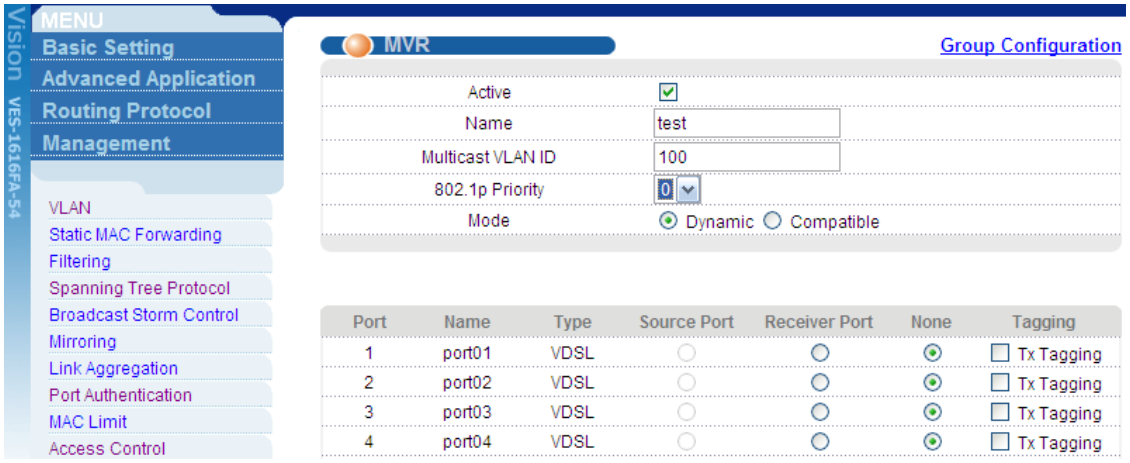


2. In the **GS-4024**, click the **Advanced Application** and then select the **VLAN.** In the **VLAN port Setting**, set the PVID of the port 10 to 100 as the multicast traffic that flows from media server to port 10 must be tagged with PVID=100 to communicate with the port in MVR VLAN 100 in VES-1616F-3X.

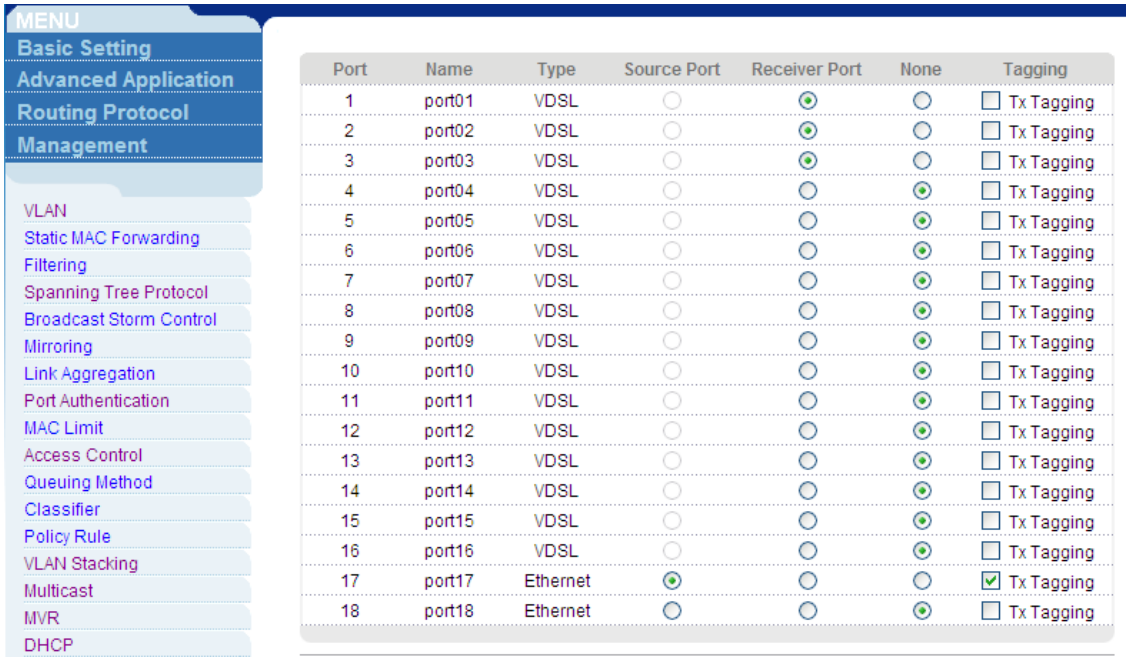
All contents copyright 2008 ZyXEL Communications Corporation.



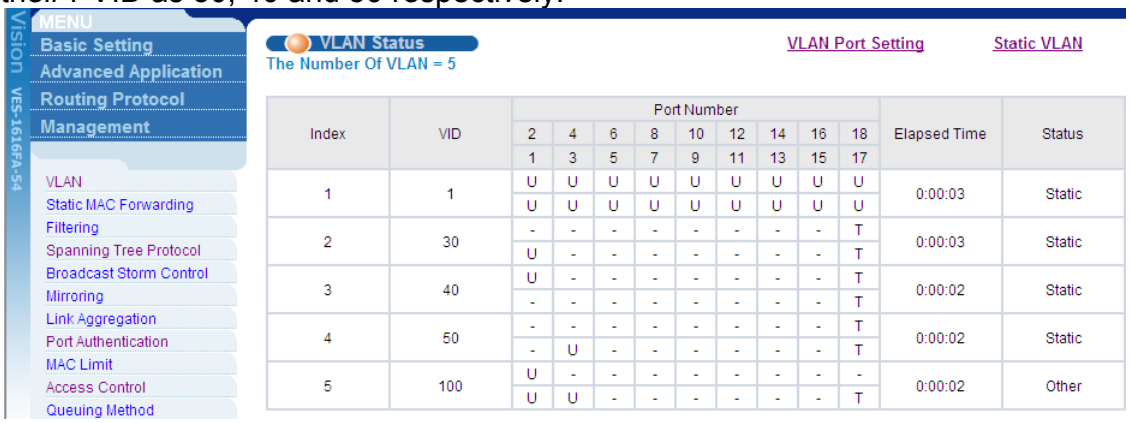
3. We need to create separate VLANs for different clients. In VES-1616FA-54, in the **Advanced Application> MVR** configure the MVR VLAN=100. Define port 1, port 2 and port 3 as the receiver ports for forwarding the multicast stream to the clients in different VLANs; set port 17 as a source port to receive traffic from the media server. Also, select mode as *dynamic* mode. The switch sends IGMP report message to multicast router through its source port.



All contents copyright 2008 ZyXEL Communications Corporation.

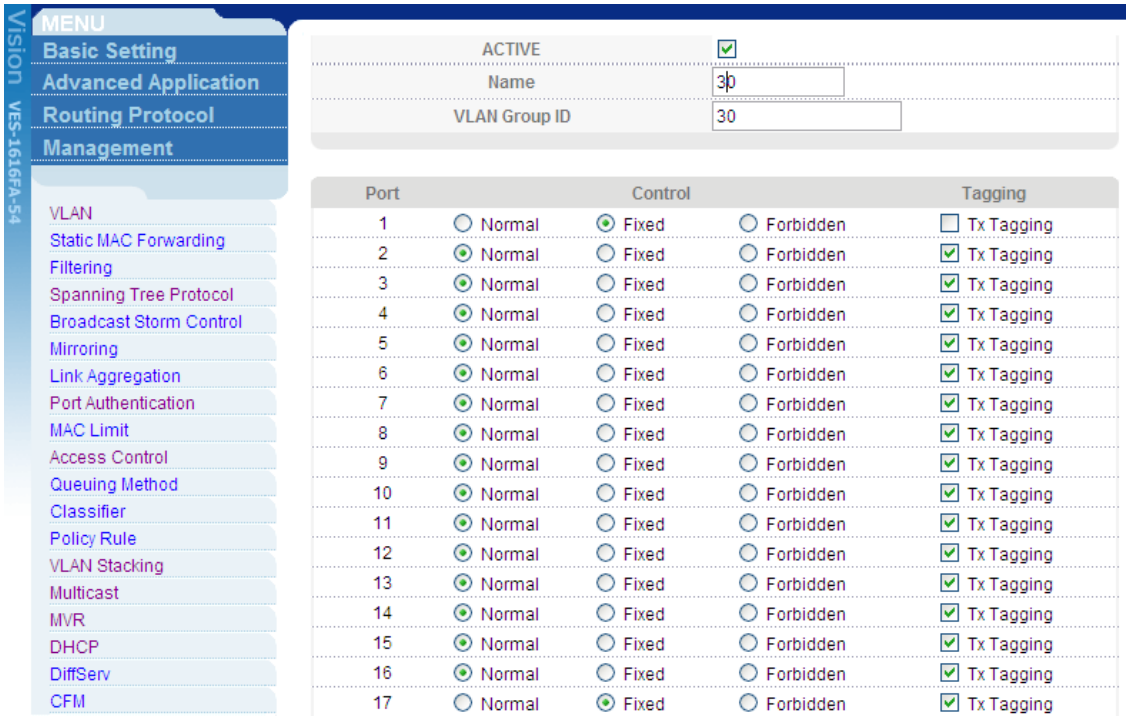


4. In **VES-1616FA-54,** after the MVR configuration, click the **Advanced Application**, **VLAN Status** and check whether there is the new VLAN 100 added in the VLAN list. We also create three separate VLANs, 30, 40, 50 and assign their PVID as 30, 40 and 50 respectively.


MENU
Basic Setting
Advanced Application
Routing Protocol
Management
VLAN
Static MAC Forwarding
Filtering
Spanning Tree Protocol
Broadcast Storm Control
Mirroring
Link Aggregation
Port Authentication
MAC Limit
Access Control
Queuing Method
VLAN Status
The Number Of VLAN = 5
VLAN Port Setting
Static VLAN
Index VID Port Number Elapsed Time Status
1 1 U U U U U U U U U U U U U U U U U 0:00:03 Static
2 30 - - - - - - - - T U - - - - - - - T 0:00:03 Static
3 40 U - - - - - - - T - - - - - - - - T 0:00:02 Static
4 50 - - - - - - - - T - U - - - - - - T 0:00:02 Static
5 100 U - - - - - - - - U U - - - - - - T 0:00:02 Other

Open Advanced Application > VLAN > Static VLAN to add a new VLAN. Tick the Active box, type VLAN Name “30” and VLAN ID “30” in the columns. Change Port 1 and Port 17 to fixed and keep port 17 tx tagging.

All contents copyright 2008 ZyXEL Communications Corporation.

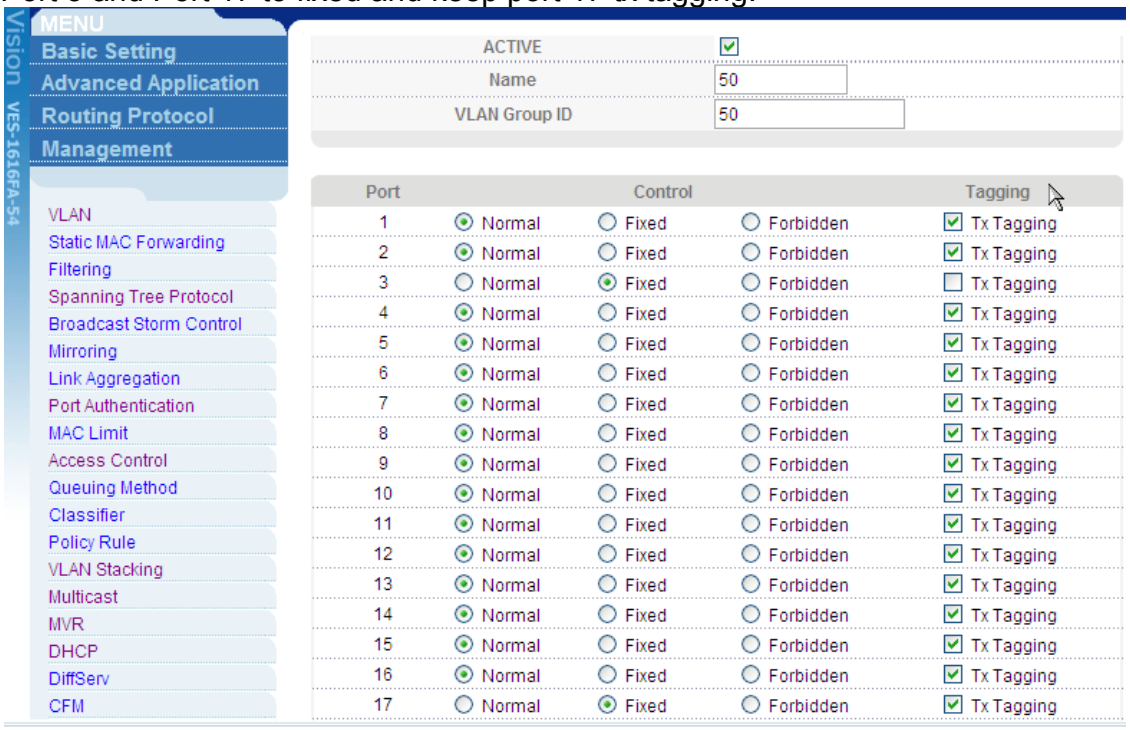


Open Advanced Application > VLAN > Static VLAN to add a new VLAN. Tick the Active box, type VLAN Name “40” and VLAN ID “40” in the columns. Change Port 2 and Port 17 to fixed and keep port 17 tx tagging.

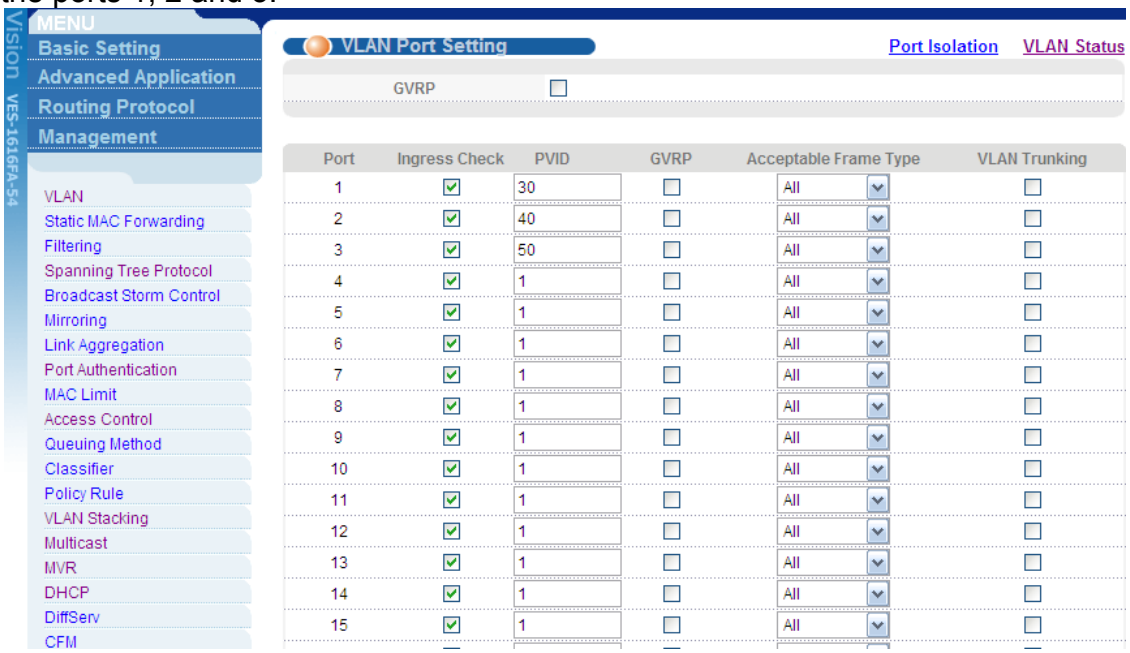
Open Advanced Application > VLAN > Static VLAN to add a new VLAN. Tick

All contents copyright 2008 ZyXEL Communications Corporation.

the Active box, type VLAN Name “50” and VLAN ID “50” in the columns. Change Port 3 and Port 17 to fixed and keep port 17 tx tagging.



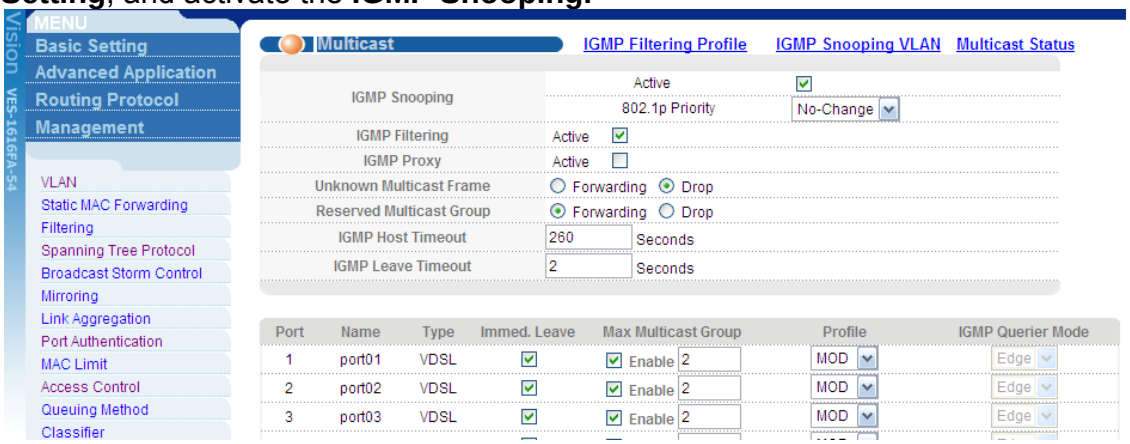
Open Advanced Application > VLAN > VLAN Port Setting to change PVID for the ports 1, 2 and 3.



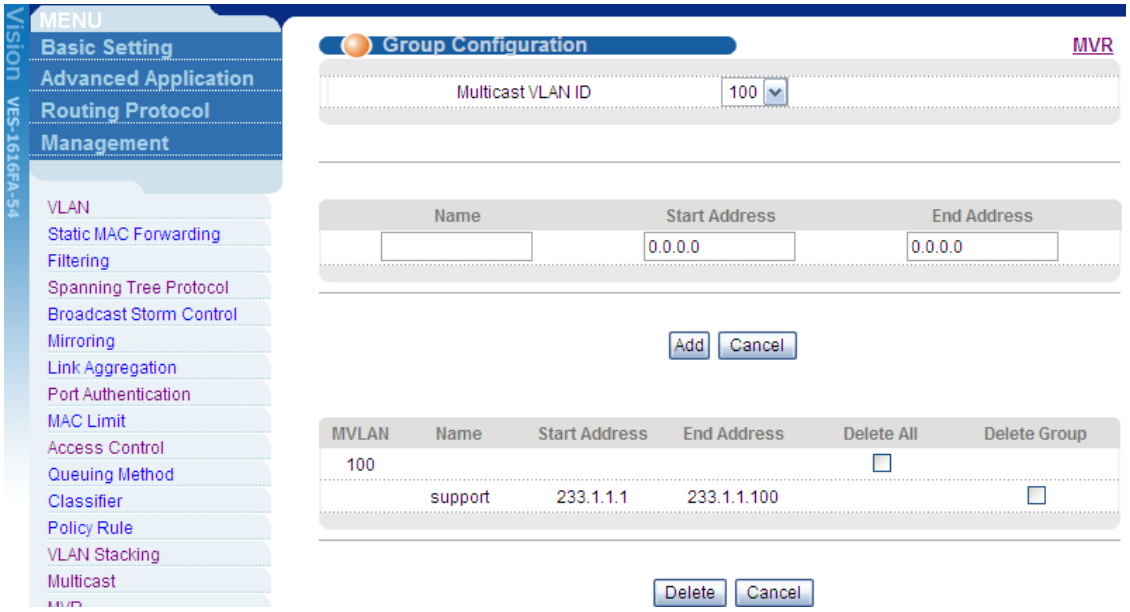
5. Before we start to use the MVR, it is fundamental to enable the IGMP Snooping first. In the VES-1616FA-54 **Menu**, click the **Multicast,** go to the **Multicast**

All contents copyright 2008 ZyXEL Communications Corporation.

Setting, and activate the **IGMP Snooping.**



7. In the **VES-1616FA-54,** go to **Advanced Application> MVR**, and then to the **Group configuration**. Set 233.1.1.1~ 233.1.1.100 as the range of multicast address so that only the clients belonging to that range of multicast group will receive the multicast traffic.



Configuration via CLI

Step 1: On the VES-1616FA-54, in the configure mode, create VLAN 100

VES-1616FA-54# config

VES-1616FA-54(config)# vlan 100

Step 2: In the VLAN 100, set the port 17 to be fixed port.

VES-1616FA-54(config-vlan)# fixed 17

Step 3: On the VES-1616FA-54, in the configure mode, create VLAN 30, and set the port 1 to be fixed port.

VES-1616FA-54(config)# vlan 30

VES-1616FA-54(config-vlan)# untagged 1

All contents copyright 2008 ZyXEL Communications Corporation.

VES-1616FA-54(config-vlan)# fixed 1

Step 4: On the VES-1616FA-54, in the configure mode, create VLAN 40, and set the port 2 to be fixed port.

VES-1616FA-54(config)# vlan 40
VES-1616FA-54(config-vlan)# untagged 2
VES-1616FA-54(config-vlan)# fixed 2

Step 5: On the VES-1616FA-54, in the configure mode, create VLAN 50, and set the port 3 to be fixed port.

VES-1616FA-54(config)# vlan 50
VES-1616FA-54(config-vlan)# untagged 3
VES-1616FA-54(config-vlan)# fixed 3

Step 6: On the VES-1616FA-54, set the PVID of specific VLAN 30

VES-1616FA-54(config)# interface port-channel 1
VES-1616FA-54(config-interface)# pvid 30
VES-1616FA-54(config-interface)# exit

Step 7: On the VES-1616FA-54, set the PVID of specific VLAN 40

VES-1616FA-54(config)# interface port-channel 2
VES-1616FA-54(config-interface)# pvid 40
VES-1616FA-54(config-interface)# exit

Step 8: On the VES-1616FA-54, set the PVID of specific VLAN 50

VES-1616FA-54(config)# interface port-channel 3
VES-1616FA-54(config-interface)# pvid 50
VES-1616FA-54(config-interface)# exit

Step 9: On the VES-1616FA-54, in the configure mode, enable IGMP snooping

VES-1616FA-54(config)#igmpsnooping

Step 10: On the VES-1616F-3X, in the configure mode, create MVR

VES-1616FA-54(config)# mvr 100

Step 11: Define the Dynamic mode

VES-1616FA-54(config-mvr)# mode dynamic

Step 12: on the VES-1616FA-54, in the MVR 100, set up the multicast group address.

VES-1616FA-54(config-mvr)# group test start-address 233.1.1.1 end-address 233.1.1.100

Step 13: In the MVR 100, specify receiver ports on port 1~3 as untagged ports

VES-1616FA-54(config-mvr)# receiver-port 1-3
VES-1616FA-54(config-mvr)# untagged 1-3

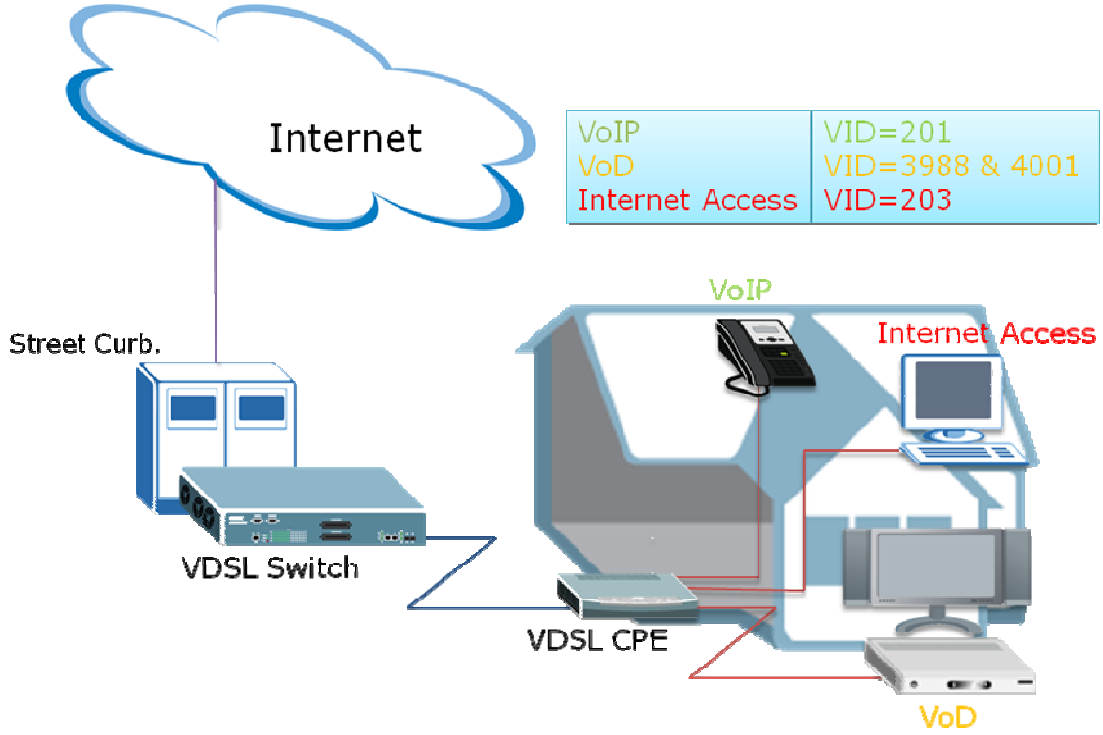
Step 14: Then, specify the source port 17 and assign it to be tagged ports

VES-1616FA-54(config-mvr)# source-port 17
VES-1616FA-54(config-mvr)# tagged 17

All contents copyright 2008 ZyXEL Communications Corporation.

Triple play Application

The triple play application is more and more popular recently, there are many methods to achieve the triple play application, and this is an example to show how to configure the VDSL modem to achieve triple play application. The network topology is shown on the figure below.
There are three kinds of service traffic flows with different VLAN ID. The VLAN ID 201 is assigned for VoIP service, VLAN ID 203 is for PPPoE traffic and VLAN 3988 is for VoD and other IP over Ethernet traffic and VLAN 4001 is multicast traffic for MoD.

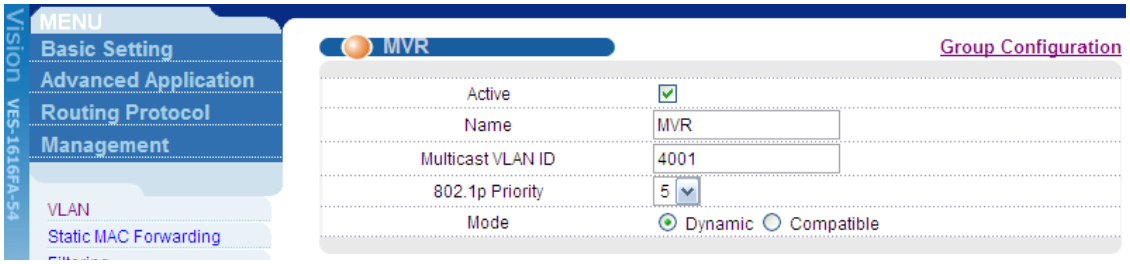


Configure VES-1616FA-54

To apply triple play, we need to enable IGMP feature in the CO side and create the VLANs to make sure all traffic flows are go through VES-1616FA-54 with correct VLAN ID.

1. Open Advanced **Application > MVR** to configure the MVR. In the MVR configuration page, check the Active checkbox to enable the MVR feature and fill in the Name and Multicast VLAN ID.

All contents copyright 2008 ZyXEL Communications Corporation.

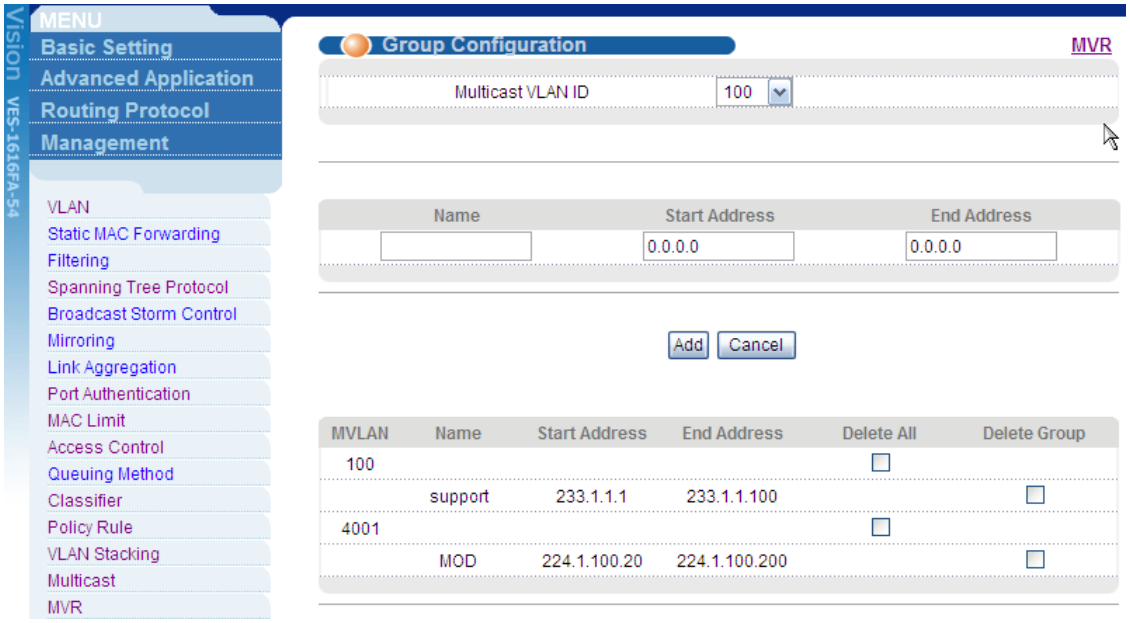


2. In the MVR configuration page, check the VDSL port 1 to receive port and port 17 to Source port and make sure the check Tx Tagging for port 1 and port 17.

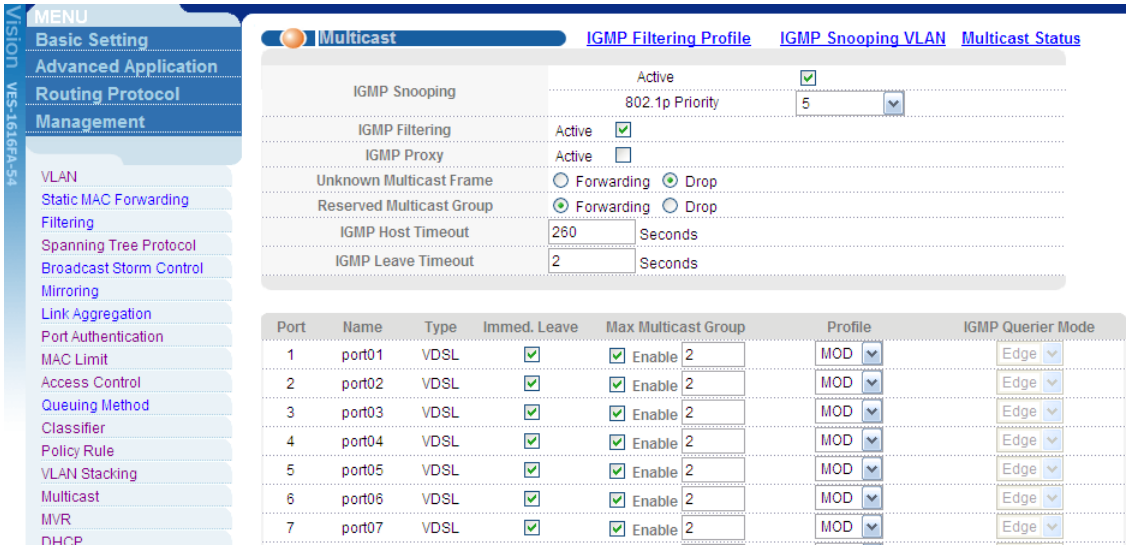
Port	Name	Type	Source Port	Receiver Port	None	Tagging
1	port01	VDSL	○	◉	○	☑ Tx Tagging
2	port02	VDSL	○	○	◉	☐ Tx Tagging
3	port03	VDSL	○	○	◉	☐ Tx Tagging
4	port04	VDSL	○	○	◉	☐ Tx Tagging
5	port05	VDSL	○	○	◉	☐ Tx Tagging
6	port06	VDSL	○	○	◉	☐ Tx Tagging
7	port07	VDSL	○	○	◉	☐ Tx Tagging
8	port08	VDSL	○	○	◉	☐ Tx Tagging
9	port09	VDSL	○	○	◉	☐ Tx Tagging
10	port10	VDSL	○	○	◉	☐ Tx Tagging
11	port11	VDSL	○	○	◉	☐ Tx Tagging
12	port12	VDSL	○	○	◉	☐ Tx Tagging
13	port13	VDSL	○	○	◉	☐ Tx Tagging
14	port14	VDSL	○	○	◉	☐ Tx Tagging
15	port15	VDSL	○	○	◉	☐ Tx Tagging
16	port16	VDSL	○	○	◉	☐ Tx Tagging
17	port17	Ethernet	◉	○	○	☑ Tx Tagging
18	port18	Ethernet	○	○	◉	☐ Tx Tagging

3. Click the Group configuration link to configure the multicast group IP. Fill in the name for MVR and the IP range start IP address is 224.1.100.20 and End Address is 224.1.100.200.

All contents copyright 2008 ZyXEL Communications Corporation.

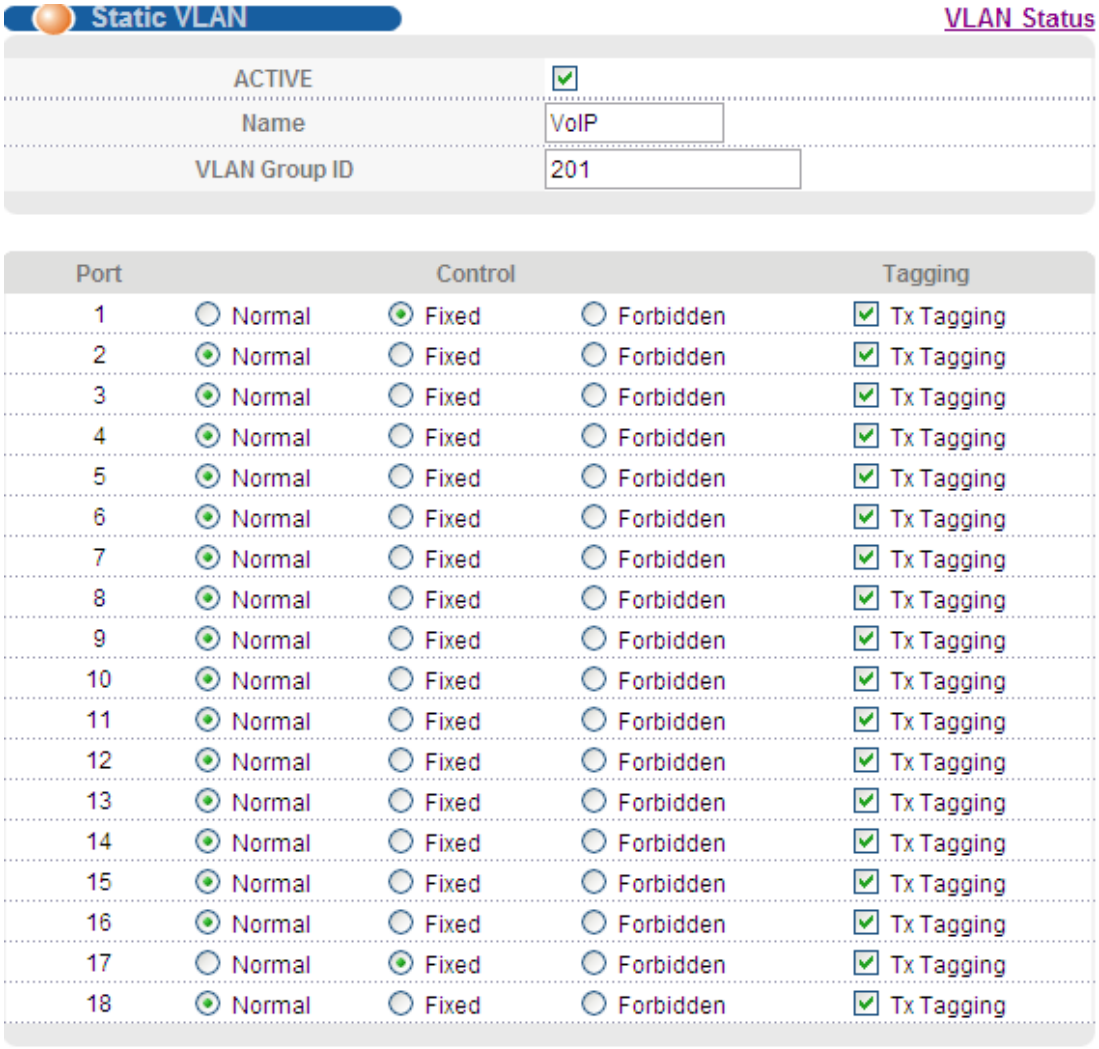


4. Open **Advanced Application > Multicast** to enable the IGMP snooping feature at the Multicast configuration page. To avoid the unknown multicast frames flooding to all VDSL ports, check the Drop to make sure the unknown multicast frames will be dropped. Click Apply button to save the settings.



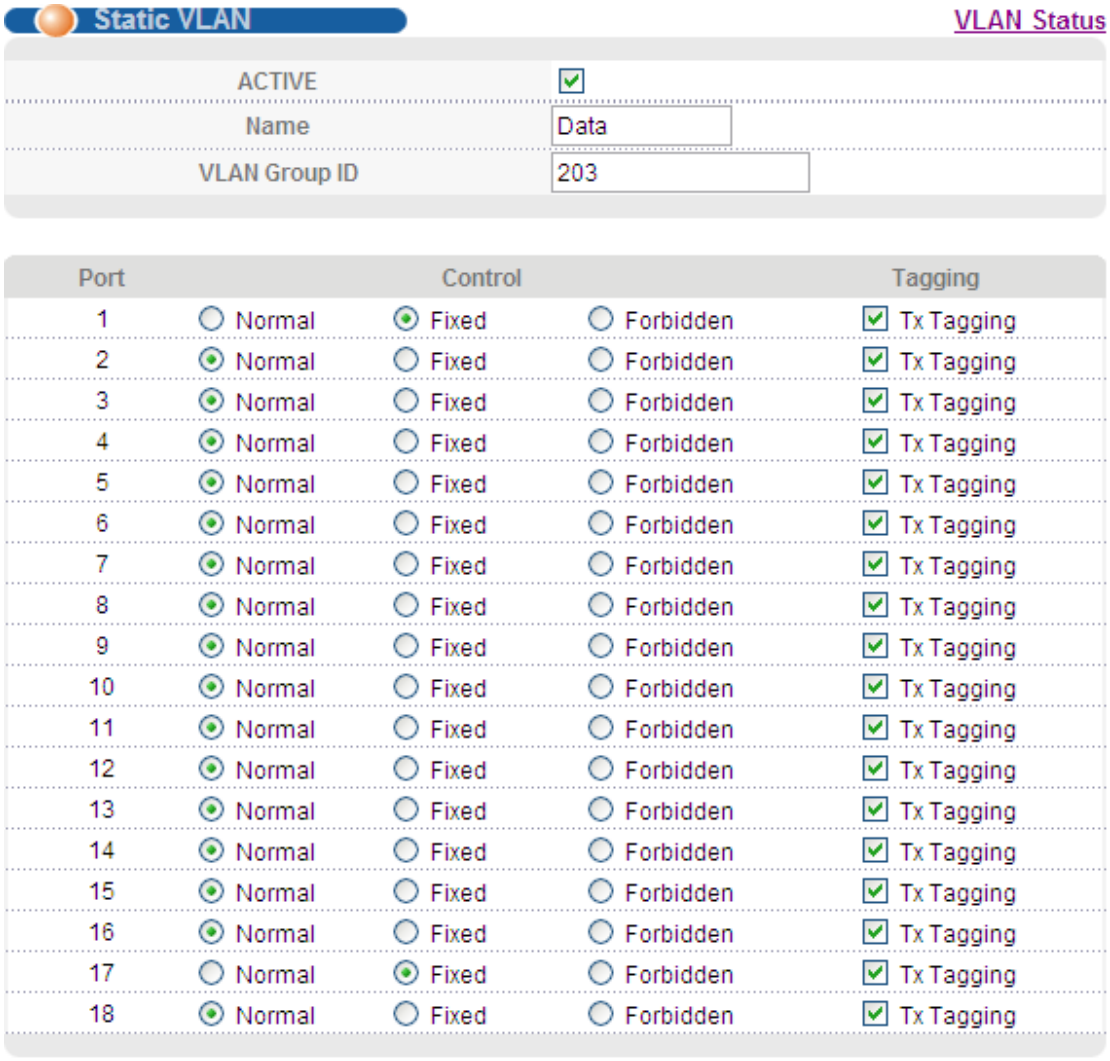
5. Open Advanced Application > VLAN and click static VLAN link to create VLAN. Check the ACTIVE checkbox to enable and fill in the VLAN name VoIP and VLAN ID 201. Configure port 1 and port 17 to Fixed and check the Tx Tagging checkbox.

All contents copyright 2008 ZyXEL Communications Corporation.


Static VLAN
VLAN Status
ACTIVE
Name
VoIP
VLAN Group ID
201
Port
Control
Tagging
1 Normal Fixed Forbidden Tx Tagging
2 Normal Fixed Forbidden Tx Tagging
3 Normal Fixed Forbidden Tx Tagging
4 Normal Fixed Forbidden Tx Tagging
5 Normal Fixed Forbidden Tx Tagging
6 Normal Fixed Forbidden Tx Tagging
7 Normal Fixed Forbidden Tx Tagging
8 Normal Fixed Forbidden Tx Tagging
9 Normal Fixed Forbidden Tx Tagging
10 Normal Fixed Forbidden Tx Tagging
11 Normal Fixed Forbidden Tx Tagging
12 Normal Fixed Forbidden Tx Tagging
13 Normal Fixed Forbidden Tx Tagging
14 Normal Fixed Forbidden Tx Tagging
15 Normal Fixed Forbidden Tx Tagging
16 Normal Fixed Forbidden Tx Tagging
17 Normal Fixed Forbidden Tx Tagging
18 Normal Fixed Forbidden Tx Tagging

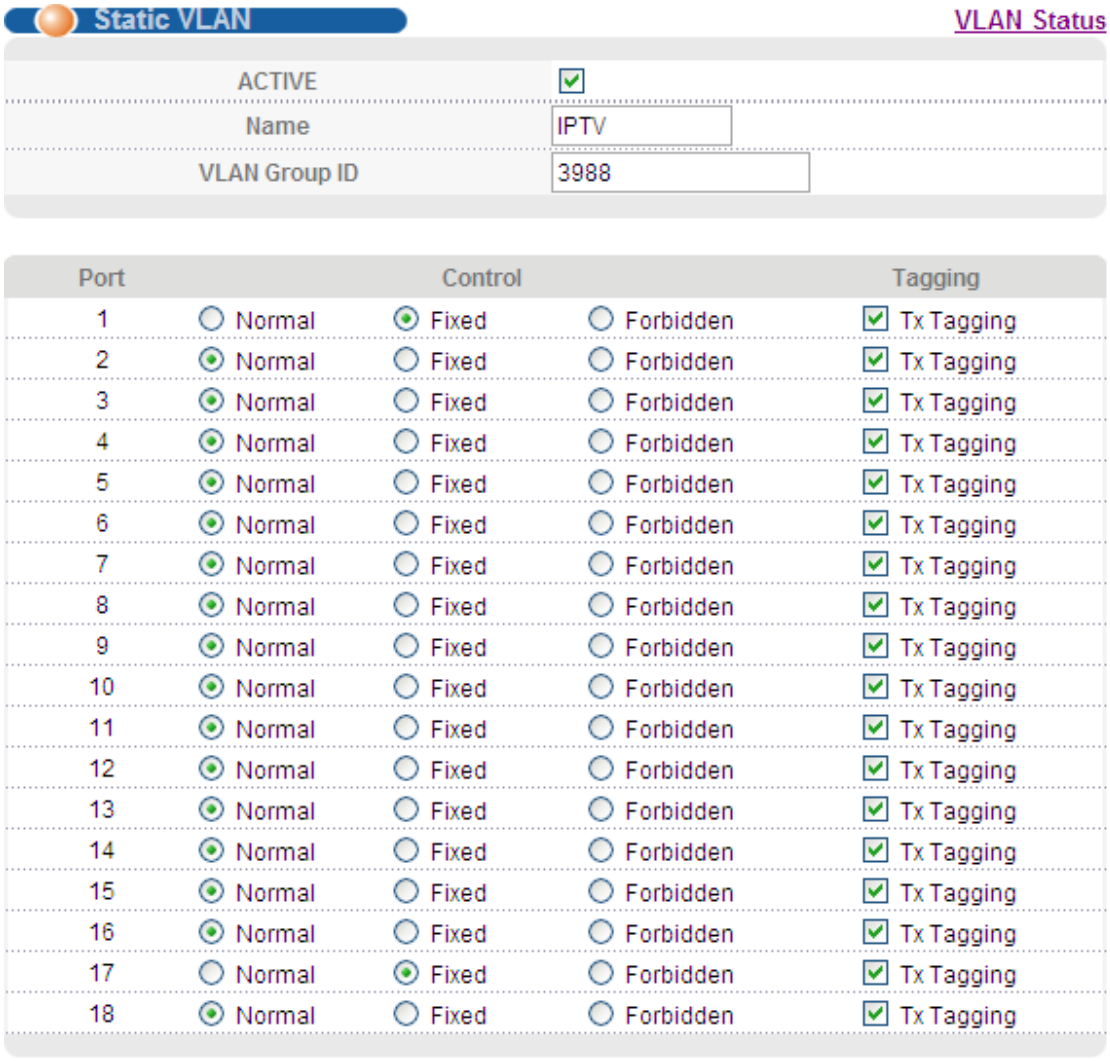
Check the ACTIVE checkbox to enable and fill in the VLAN name Data and VLAN ID 203. Configure port 1 and port 17 to Fixed and check the Tx Tagging checkbox.

All contents copyright 2008 ZyXEL Communications Corporation.


Static VLAN
VLAN Status
ACTIVE
Name
Data
VLAN Group ID
203
Port
Control
Tagging
1 Normal Fixed Forbidden Tx Tagging
2 Normal Fixed Forbidden Tx Tagging
3 Normal Fixed Forbidden Tx Tagging
4 Normal Fixed Forbidden Tx Tagging
5 Normal Fixed Forbidden Tx Tagging
6 Normal Fixed Forbidden Tx Tagging
7 Normal Fixed Forbidden Tx Tagging
8 Normal Fixed Forbidden Tx Tagging
9 Normal Fixed Forbidden Tx Tagging
10 Normal Fixed Forbidden Tx Tagging
11 Normal Fixed Forbidden Tx Tagging
12 Normal Fixed Forbidden Tx Tagging
13 Normal Fixed Forbidden Tx Tagging
14 Normal Fixed Forbidden Tx Tagging
15 Normal Fixed Forbidden Tx Tagging
16 Normal Fixed Forbidden Tx Tagging
17 Normal Fixed Forbidden Tx Tagging
18 Normal Fixed Forbidden Tx Tagging

Check the ACTIVE checkbox to enable and fill in the VLAN name IPTV and VLAN ID 3988. Configure port 1 and port 17 to Fixed and check the Tx Tagging checkbox.

All contents copyright 2008 ZyXEL Communications Corporation.


Static VLAN
VLAN Status
ACTIVE
Name
IPTV
VLAN Group ID
3988
Port
Control
Tagging
1 Normal Fixed Forbidden Tx Tagging
2 Normal Fixed Forbidden Tx Tagging
3 Normal Fixed Forbidden Tx Tagging
4 Normal Fixed Forbidden Tx Tagging
5 Normal Fixed Forbidden Tx Tagging
6 Normal Fixed Forbidden Tx Tagging
7 Normal Fixed Forbidden Tx Tagging
8 Normal Fixed Forbidden Tx Tagging
9 Normal Fixed Forbidden Tx Tagging
10 Normal Fixed Forbidden Tx Tagging
11 Normal Fixed Forbidden Tx Tagging
12 Normal Fixed Forbidden Tx Tagging
13 Normal Fixed Forbidden Tx Tagging
14 Normal Fixed Forbidden Tx Tagging
15 Normal Fixed Forbidden Tx Tagging
16 Normal Fixed Forbidden Tx Tagging
17 Normal Fixed Forbidden Tx Tagging
18 Normal Fixed Forbidden Tx Tagging

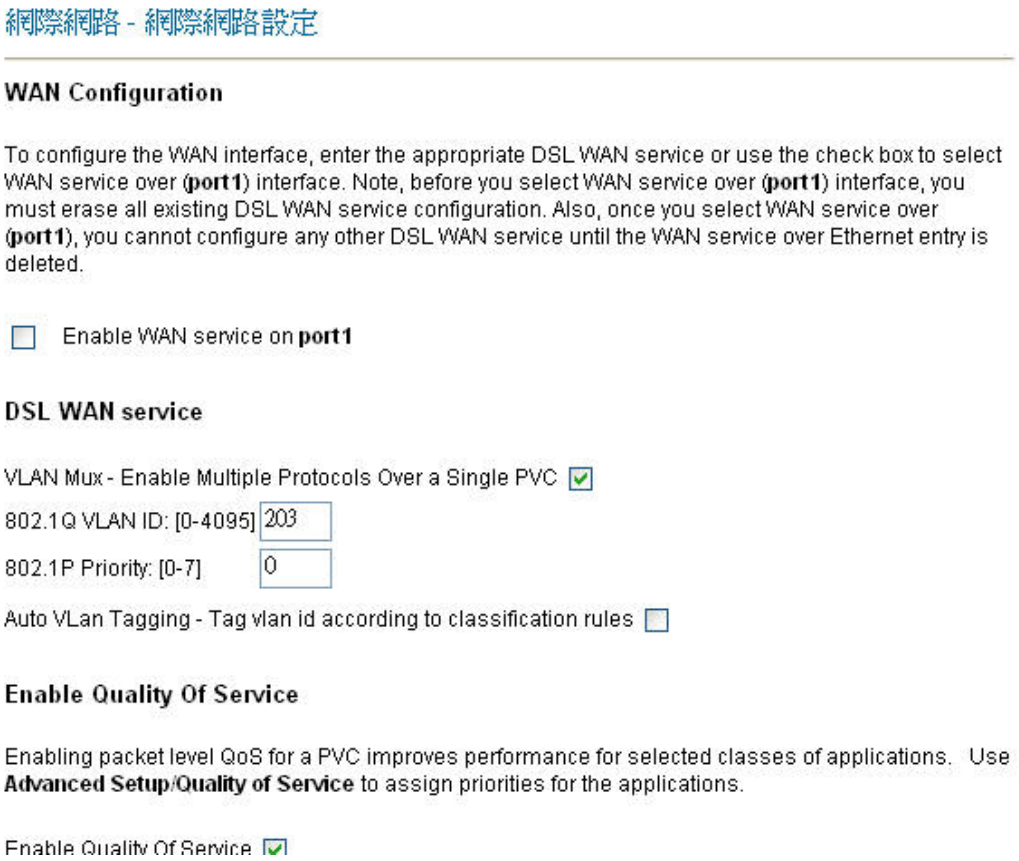
Configure P-870H-51

According to the figure shown above, we need to create different WAN interfaces in the VDSL modem for different traffic flows and also we need to create classification rule to identify these different traffic flows. In this document, we will use P-870H-51 for the configuration example.
The management IP address of P-870H-51 is 192.168.1.1.After logging in; the first step is to create WAN Interface.

1. Create WAN Interface via WEB GUI.

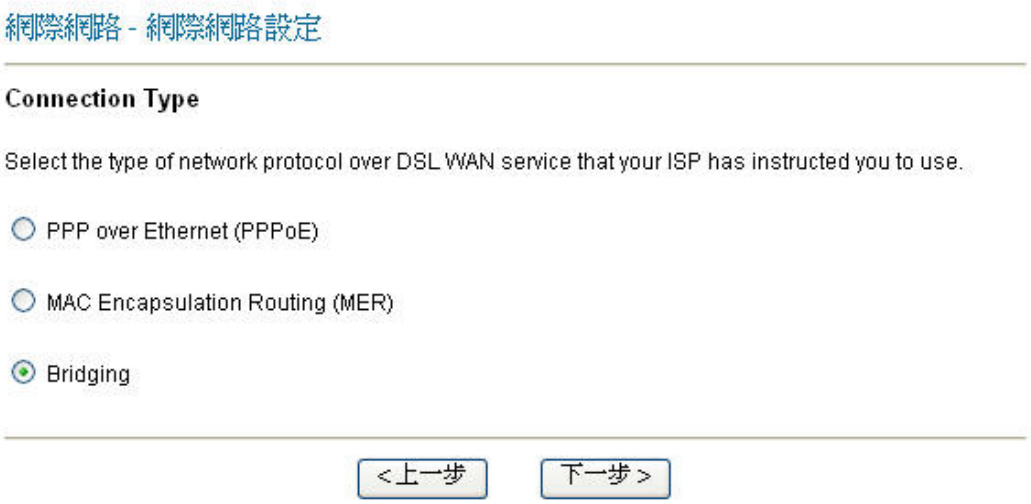
All contents copyright 2008 ZyXEL Communications Corporation.

Open Advanced Setup > WAN to Create new WAN Interface. First click the add button to add a new interface. Then check the VLAN Mux option to enable the IEEE 802.1Q VLAN on this Interface and fill in the VLAN ID. Click the Enable Quality of Service option to enable QoS feature on P-870H-51 then click the next button to move to the next step.

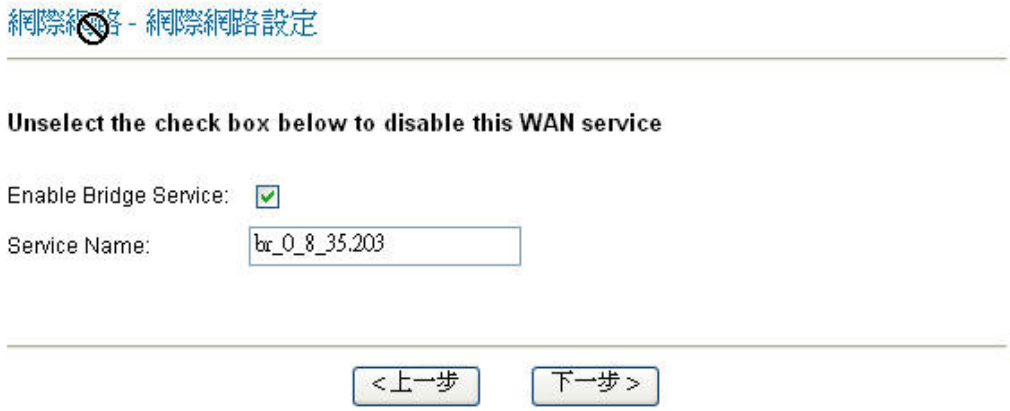

網際網路 - 網際網路設定
WAN Configuration
To configure the WAN interface, enter the appropriate DSL WAN service or use the check box to select WAN service over (port1) interface. Note, before you select WAN service over (port1) interface, you must erase all existing DSL WAN service configuration. Also, once you select WAN service over (port1), you cannot configure any other DSL WAN service until the WAN service over Ethernet entry is deleted.
Enable WAN service on port1
DSL WAN service
VLAN Mux - Enable Multiple Protocols Over a Single PVC
802.1Q VLAN ID: [0-4095] 203
802.1P Priority: [0-7] 0
Auto VLan Tagging - Tag vlan id according to classification rules
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service

In the connection type configuration page, select Bridging mode and click the next button to move to the next configuration step.

All contents copyright 2008 ZyXEL Communications Corporation.


網際網路 - 網際網路設定
Connection Type
Select the type of network protocol over DSL WAN service that your ISP has instructed you to use.
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
Bridging
<上一步
下一步>

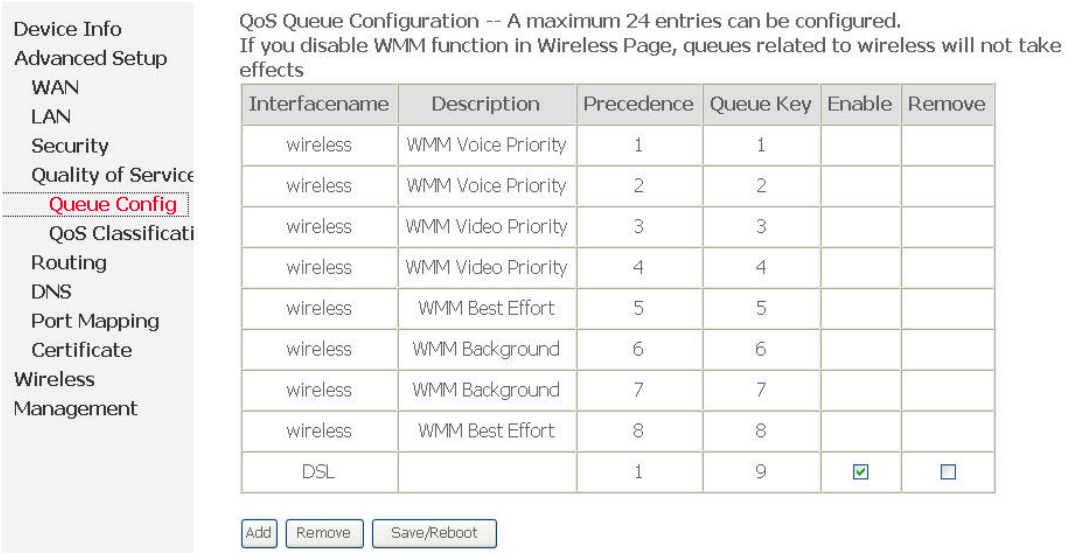
The next step is to modify the WAN interface name. Then click the next button to move to the next configuration step page.



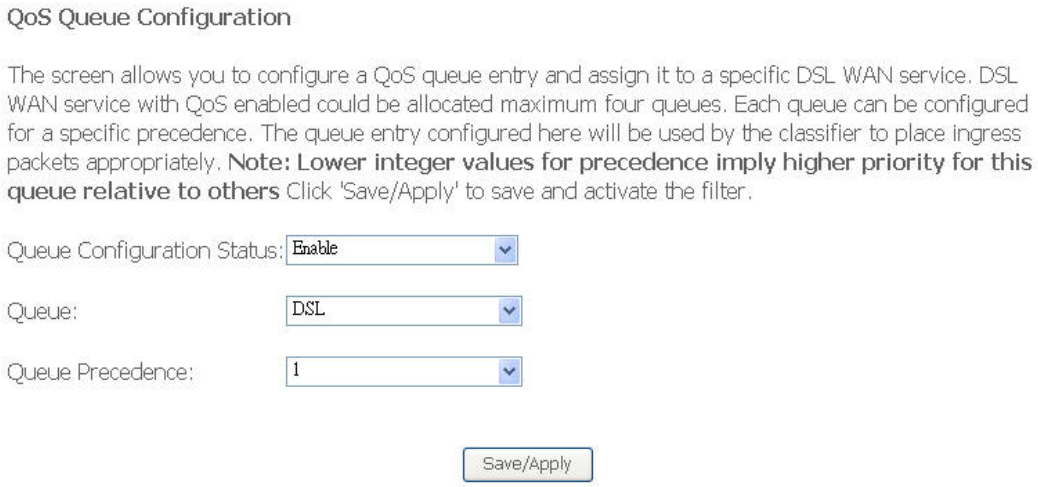
The last is the confirmation page, click the save button to save and finish the process of creating the WAN interface. Repeat the above steps to create the other three interfaces with the VLAN ID 201, 3988 and 4001.

2. Create a Queue for the WAN Interface via WEB GUI.
Open Advance Setup > Queue Config and click the Add button to open the QoS Queue configuration page.

All contents copyright 2008 ZyXEL Communications Corporation.



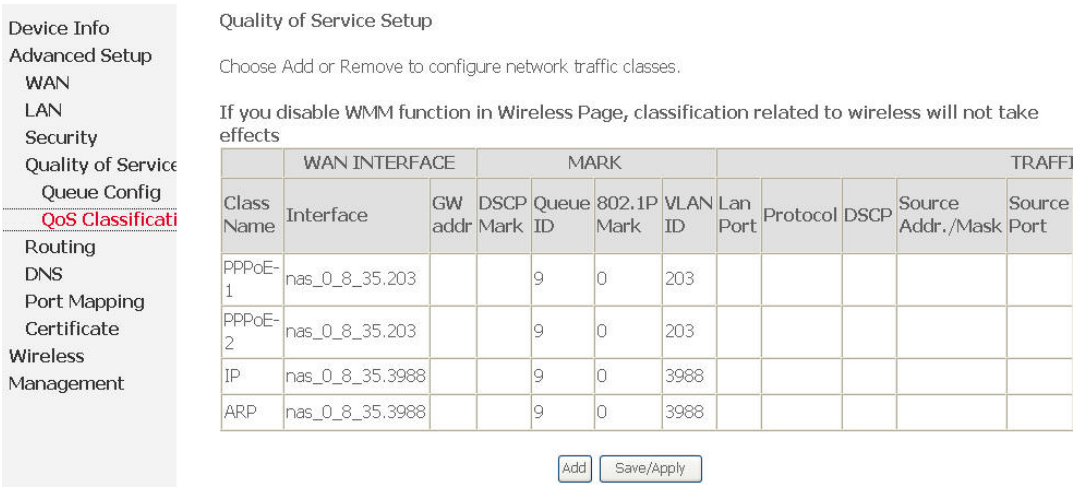
In the QoS Queue Configuration page, create a new Queue like on the figure below and click the Save/Apply button to finish and save the settings.


QoS Queue Configuration
The screen allows you to configure a QoS queue entry and assign it to a specific DSL WAN service. DSL WAN service with QoS enabled could be allocated maximum four queues. Each queue can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. Note: Lower integer values for precedence imply higher priority for this queue relative to others Click 'Save/Apply' to save and activate the filter.
Queue Configuration Status: Enable
Queue: DSL
Queue Precedence: 1
Save/Apply

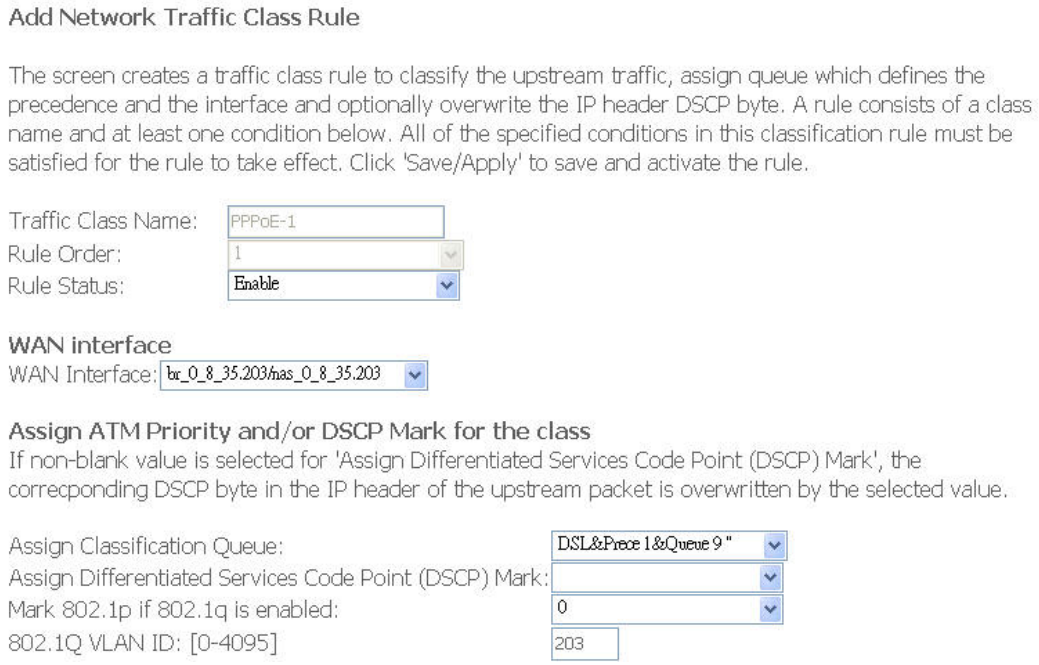
After finishing the process of creating the WAN interfaces and Queue, click the Save/Reboot button on the Queue Config page to save the above settings and reboot the device for the changes to take effect.

3. Configuration the QoS classification to classify traffic flow.
Open Advanced Setup > QoS Classification page to classify traffic flow. Click ADD button to add a new classification rule, in this document, we need create classification rules to identify and classify the PPPoE, IPoE and VoIP traffic flows.

All contents copyright 2008 ZyXEL Communications Corporation.



In the Add Network Traffic Class Rule page, we can give each rule a name for easy identification, for example PPPoE-1, PPPoE-2, IP, ARP and VoIP. Assign the order for each rule and check the Enable option to make sure this rule is enabled. We need to define that this kind of traffic will be sent through a specific WAN interface, in other words, that it would be added the VLAN ID when sent through this WAN Interface, and that is why we enable the VLAN Mux. For example, the PPPoE-1 and PPPoE-2 need to be added the VLAN ID 203, we select the WAN interface which will add the VLAN ID 203 for these two rules. Scroll down the page to configure the other parameters.

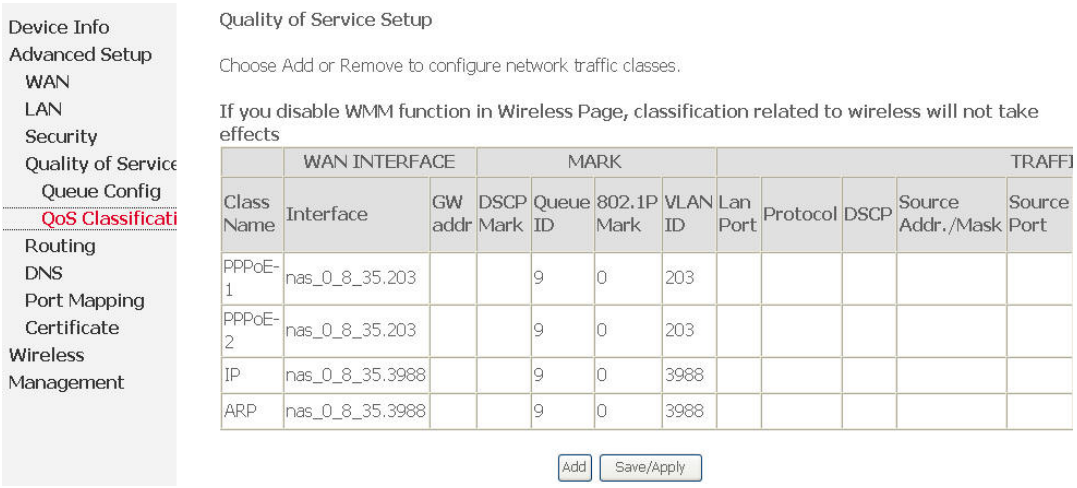

Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name:
PPPoE-1
Rule Order:
1
Rule Status:
Enable
WAN interface
WAN Interface:
br_0_8_35.203/nas_0_8_35.203
Assign ATM Priority and/or DSCP Mark for the class
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.
Assign Classification Queue:
DSL&Prece 1&Queue 9 "
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled:
0
802.1Q VLAN ID: [0-4095]
203

On this page, there are two sets of the traffic parameters used to define the traffic. In the section of SET-1, we can base on the layer 3 parameters and SET-2 is the protocol type. In this case, we will use protocol type to class PPPoE and IPoE (IP and ARP). There are two types of protocols for PPPoE (8863 and 8864); the Hex

All contents copyright 2008 ZyXEL Communications Corporation.

code for IP is 0800, ARP is 0806.
Click Save/Apply button to save and finish the process of creating a new network traffic class rule.

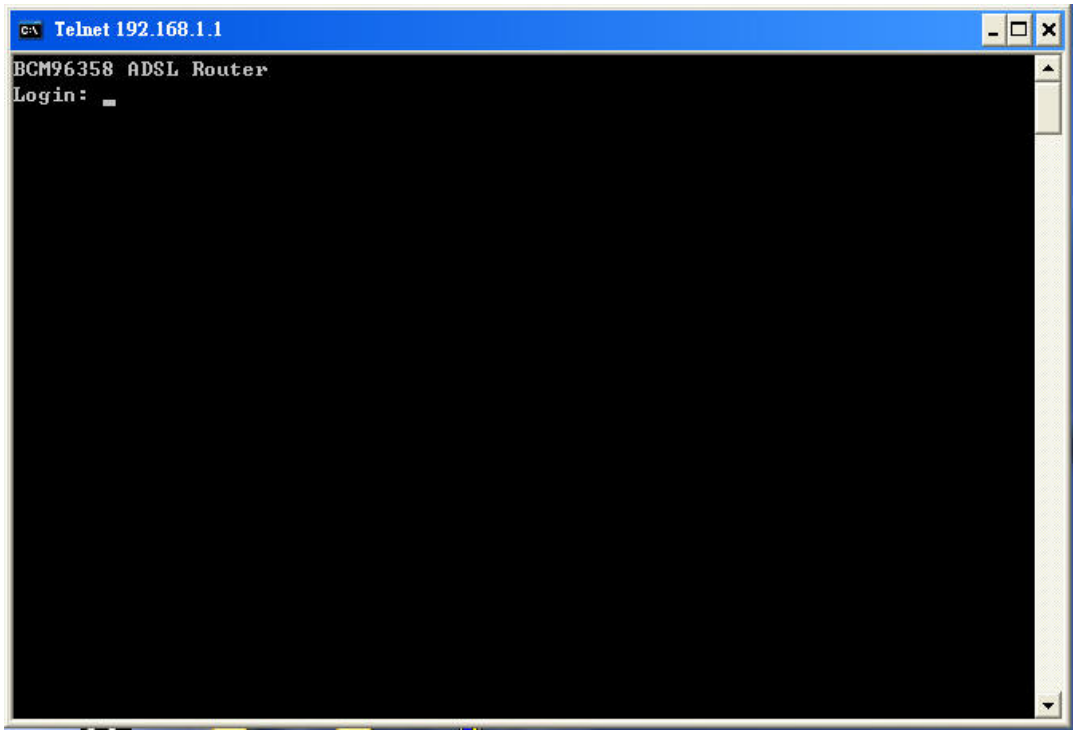
Repeat the above steps to create the classification rule for PPPoE, IPoE and VoIP.



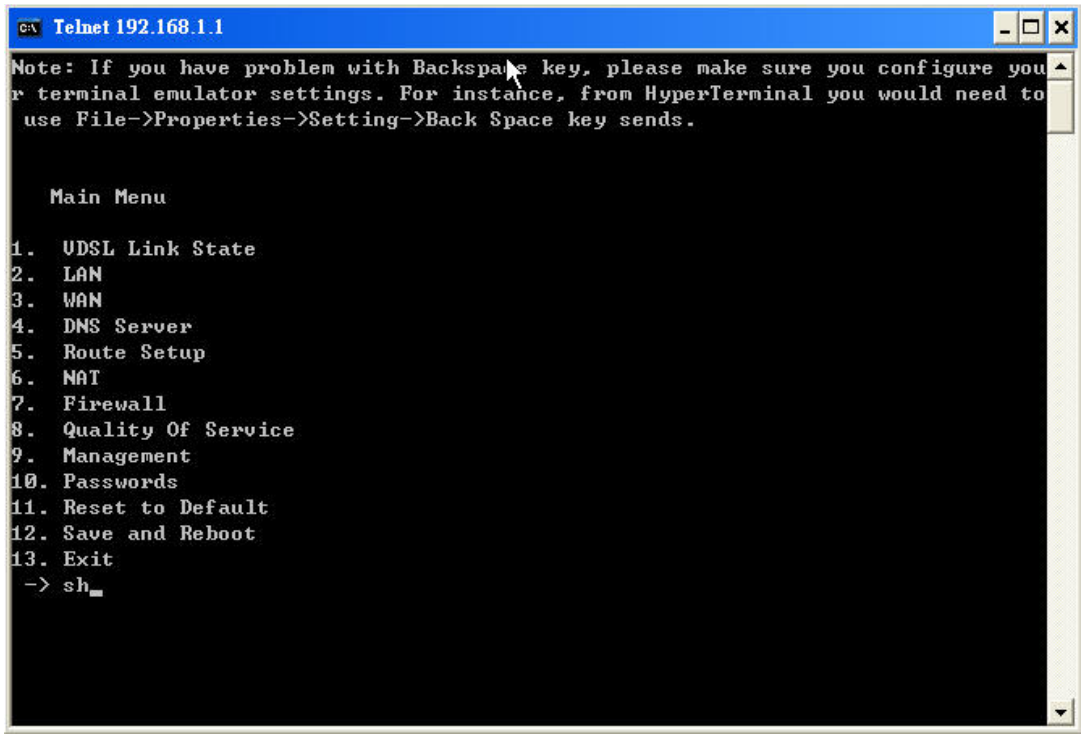
In this case, we will fix the VoIP service at the Ethernet port 4 and remaining ports for other services. Therefore we will need use CLI command to configure the port based VLAN setting which will combine all traffic from the Ethernet port 4 of P-870H-51 with the VLAN ID 201. To make sure the CLI command works properly, we need to make sure the order of rule for the VLAN 201 is 1. This should help us to make sure the CLI command can map to the correct WAN interface with correct VLAN ID.
Click the Save/Apply button at the QoS classification page to save and finish all the settings related to WEB GUI since we will use CLI commands to finish all the other settings.

4. Configure the port based VLAN through Telnet or Console port. Connect the CLI mode of P-870H-51 through Telnet session or console UI. In this case, we will use Telnet session to show how to configure the CLI command.

All contents copyright 2008 ZyXEL Communications Corporation.



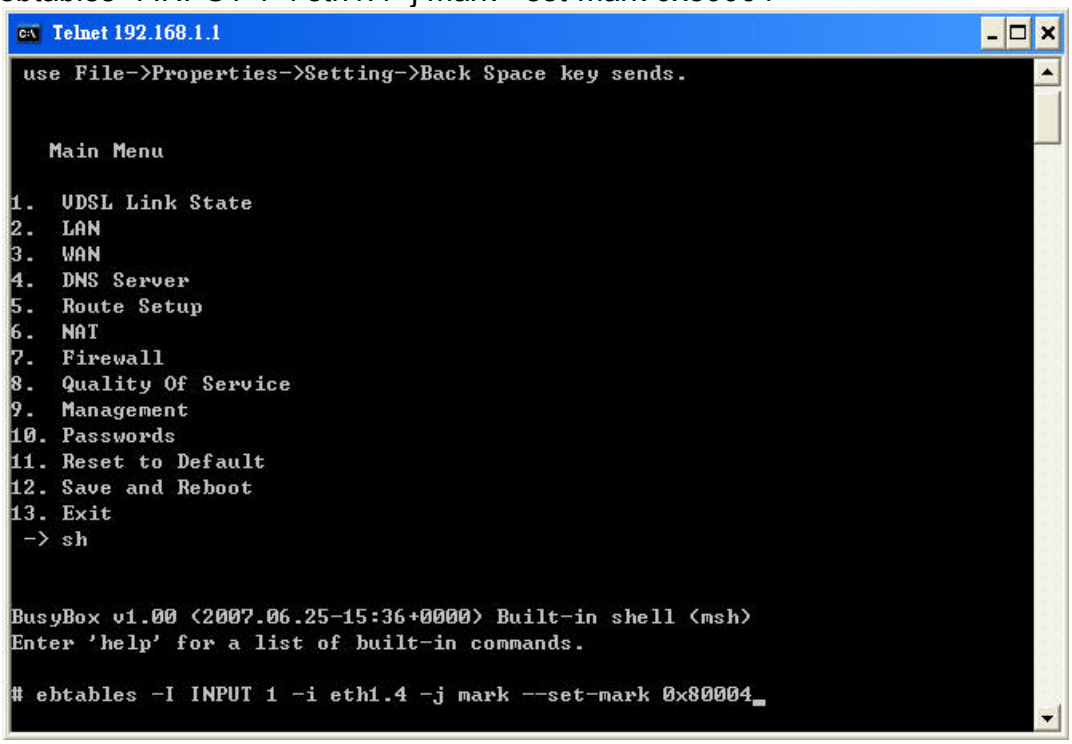
After logging in the CLI of P-870H-51, we can see the picture below showing the list of the commands and other information. Type sh command to enter the CLI mode.


Telnet 192.168.1.1
Note: If you have problem with Backspace key, please make sure you configure your terminal emulator settings. For instance, from HyperTerminal you would need to use File->Properties->Setting->Back Space key sends.
Main Menu
1. VDSL Link State
2. LAN
3. WAN
4. DNS Server
5. Route Setup
6. NAT
7. Firewall
8. Quality Of Service
9. Management
10. Passwords
11. Reset to Default
12. Save and Reboot
13. Exit
-> sh

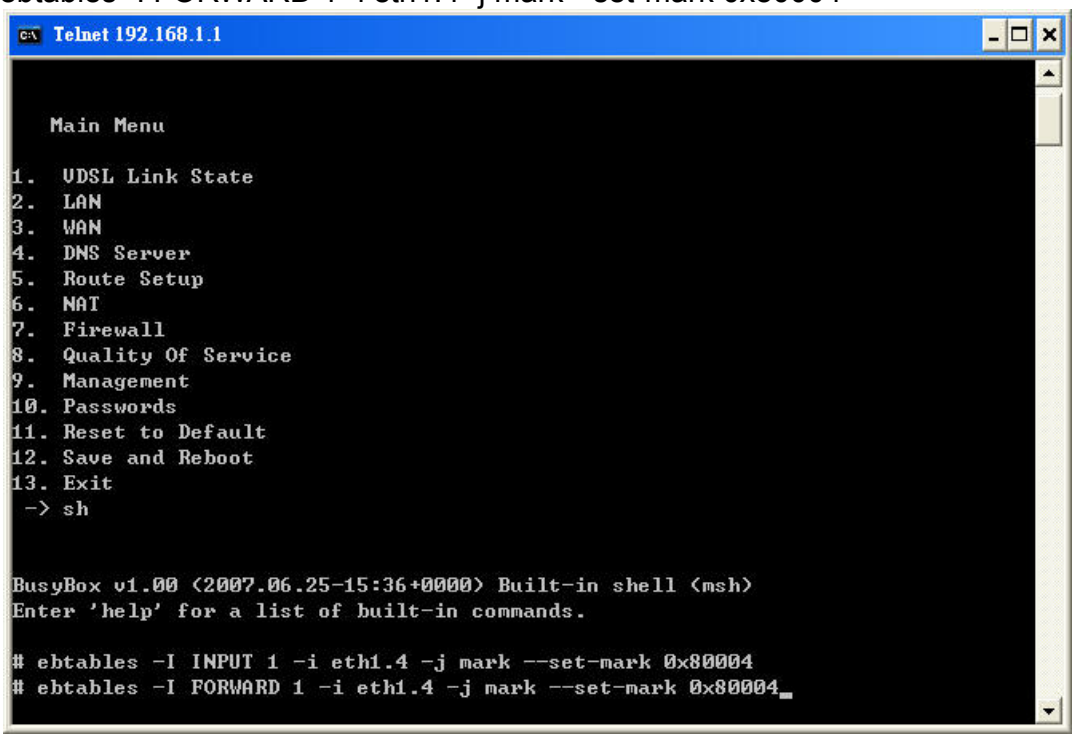
After that, enter the below commands to configure the port based VLAN settings.

All contents copyright 2008 ZyXEL Communications Corporation.

ebtables -I INPUT 1 -i eth1.4 -j mark --set-mark 0x80004



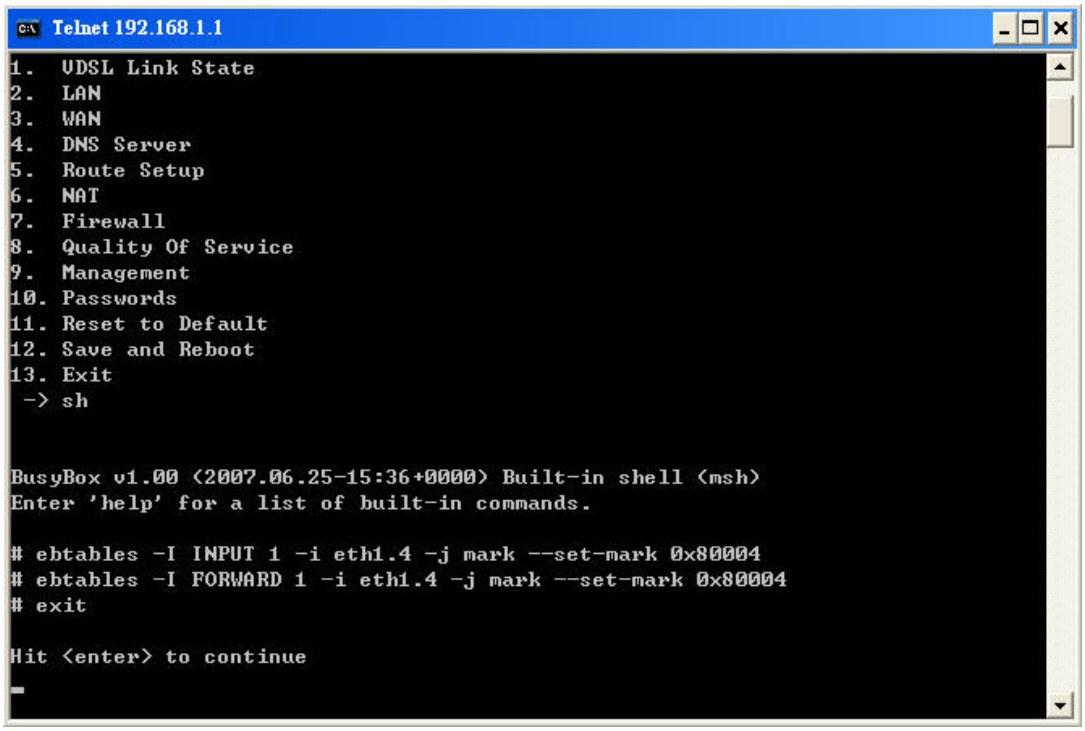
The second command is：
ebtables -I FORWARD 1 -i eth1.4 -j mark --set-mark 0x80004



After issuing these two commands, the settings are done. Type exit to exit the CLI

All contents copyright 2008 ZyXEL Communications Corporation.

mode.



We finished all the settings to use P-870H-51 to classify the service flows. Let's review what we done: we classified the traffic for VoIP, PPPoE for Internet Access and IPoE for VoD. With these settings, P-870H-51 can work as a home gateway to help service provider to provide VoIP service to customer at the Ethernet port 4 and Internet access and IPTV service on the remaining ports.

All contents copyright 2008 ZyXEL Communications Corporation.

Ringing a network by building redundant

links and connections between Switch

What is Spanning Tree Protocol?

Spanning Tree Overview

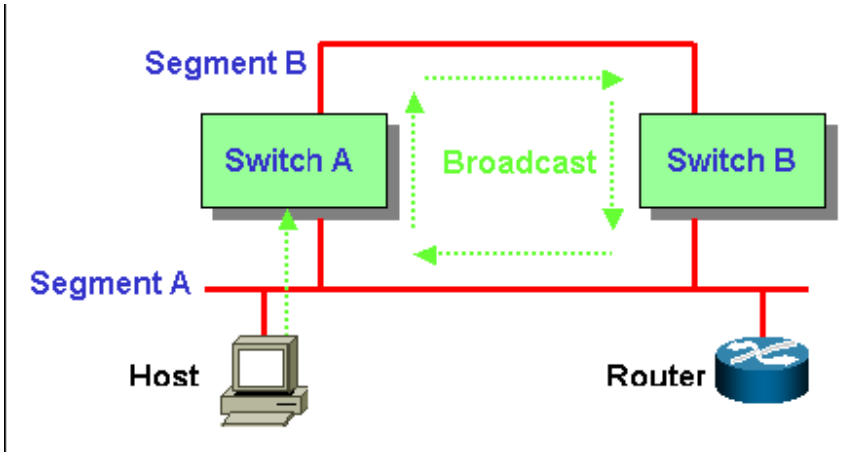
Spanning-Tree Protocol (STP) is a Layer 2 protocol designed to run on the bridges and the switches. The specification for STP is defined in IEEE 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. STP detects/disables network loops and provides backup links between switches or bridges. It allows the device to interact with other STP compliant devices in your network to ensure that only one path exists between any two stations on the network.
The redundant topology without STP will cause the following problem:

1. Broadcast storm:

Without Spanning Tree loop avoidance mechanism, each switch will endlessly flood broadcast packets to all ports. This situation is called broadcast storm.

- When Host sends a broadcast frame, like an ARP request to Router, the frame will be received by Switch A.
- Switch A identifies the destination MAC address field (broadcast FF:FF:FF:FF:FF:FF) in the frame and determine to flood it onto Segment B.
- When the broadcast frame arrives at Switch B, the switch will repeat above process, flood it to Segment A.
- The broadcast frame will endlessly travel around the loop network even id the router has already received this frame.

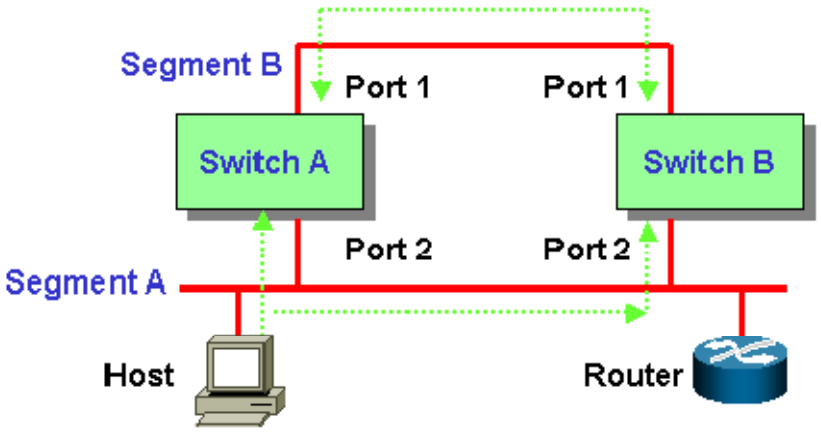
All contents copyright 2008 ZyXEL Communications Corporation.



2. Filtering Database Instability:

When multiple copies of a frame arrive at different ports of a switch, the MAC entry instability in Filtering Database will occur.

- Host sends a unicast frame to a router (source MAC address is host's MAC, destination MAC address is Router's MAC). Both Switch A and Switch B will receive this frame and learn the MAC address of the host on Port 2.
- Switch A has not yet learned the MAC address of Router. So Switch A will flood a copy of the received frame to Segment B.
- When the copy of the frame from Switch A arrives at Switch B, Switch B will remove the first entry (Host MAC address on Port 2) in Filtering Database and add a new mapping of Host MAC address on Port 1. Switch B incorrectly learn Host MAC address on Port 1.
- Switch B can't forward the frames properly because the instability of mapping MAC address to Port.



How STP Works

Spanning Tree provides a loop-free network. When a switch supporting STP recognizes a loop in the network topology, it blocks one or more redundant ports.

All contents copyright 2008 ZyXEL Communications Corporation.

Spanning Tree Protocol continually explores the network, so when the network topology changes, STP automatically reconfigures the switch ports in order to avoid the failure by blocking certain port.
Spanning tree algorithm aware switches (bridges) exchange configuration messages periodically. The configuration message is a multicast frame called BPDU (Bridge Protocol Data Unit) or Hello message. According to BPDU, these STP aware switches (bridges) will construct a loop free network with a "tree" architecture.
STP operation is described below:

1. Select a root bridge

Only one switch/ bridge can be selected as the root bridge in a given network. All other decisions in the network, such as which port is blocked and which port is put in forwarding mode, are made regarding this root bridge. The root bridge is the "root" of the constructed "tree".

- One of the important fields included in the BPDU is the bridge ID.
  Each bridge has unique bridge ID. The root bridge is the bridge with the lowest bridge ID in the spanning tree network.
- The bridge ID includes two parts, bridge priority (2 bytes) and bridge MAC address (6 bytes). The 802.1d default bridge priority is 32768. E.g. for a switch with default priority 32768 (8000 hex), MAC address is 00:A0:C5:12:34:56, its bridge ID is 8000:00A0:C512:3456.
- On the root bridge, all its ports are **designated ports**. **Designated ports are always in the forwarding state**. While in forwarding state, port can receive and send traffic.

2. Select a root port for the non-root bridge

For the non-root switch/bridge, there will be one root port. The root port is the port through which this non-root switch / bridge communicates with the root bridge (the "leaf" side of the "tree").

- The root port is the port on the non-root bridge with the lowest path cost to the root bridge. **The root port is normally in forwarding state**.
- Path cost is the total cost of transmitting a frame on to a LAN through that port to bridge root. It is assigned according to the bandwidth of the link. The slower the media, the higher the cost.
  Some of the path costs specified in the IEEE 802.1d specification are listed below.

All contents copyright 2008 ZyXEL Communications Corporation.

Link Speed	Recommended Cost	Recommended Cost Range
4Mbps	250	100 to 1000
10Mbps	100	50 to 600
16Mbps	62	40 to 400
100Mbps	19	10 to 60
1Gbps	4	3 to 10
10Gbps	2	1 to 5

- 3. When multiple ports have the same path cost to root bridge, **the port with lowest port priority is selected as root port**.

3. Select a designated port on each segment

For each LAN segment (collision domain), there is a designated port. The designated port has the lowest cost to the root bridge. Designated ports are normally in the forwarding state to forward and receive traffic to the segment. If more than one port in the segment have the same path cost, the port on which bridge has the lowest bridge ID is selected as a designated port.

How STP works

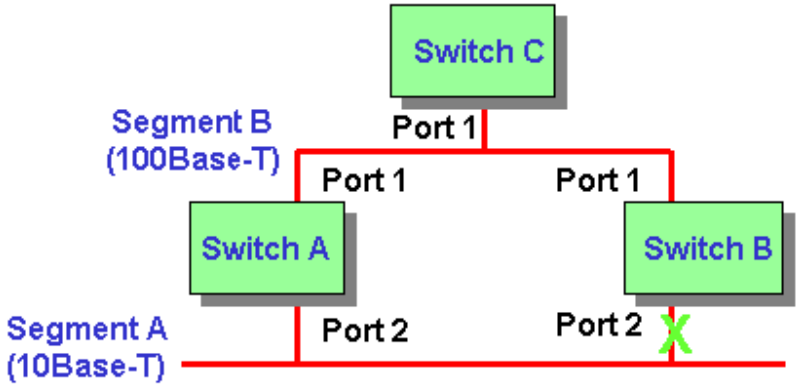
After STP determines the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops. STP-aware devices exchange Bridge Protocol Data Units (BPDUs) periodically. Whenever the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

For example:

All contents copyright 2008 ZyXEL Communications Corporation.

Switch A: MAC = 00A0C5111111, Priority = 32768			**Switch B:** MAC = 00A0C5222222, Priority = 32768			**Switch C:** MAC = 00A0C5333333 Priority = 1	
	Port 1	Port 2		Port 1	Port 2		Port 1
Cost	19	100	Cost	19	100	Cost	19
Priority	128	128	Priority	128	128	Priority	128



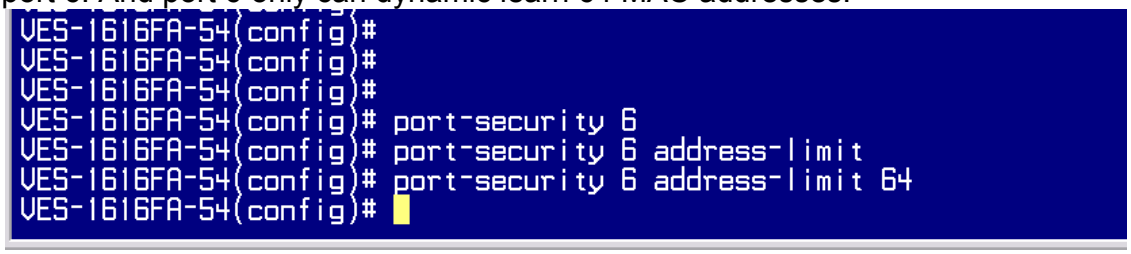
1. Switch A bridge ID = 8000:00A0:C511:1111, Switch B bridge ID = 8000:00A0:C522:2222, Switch C bridge ID = 0001:00A0:C533:3333. Switch C has the lowest bridge ID, so Switch C is the root bridge. All ports of the root bridge are designated ports, so Port 1 is designated port.
2. For non-root bridge Switch A, Port 1 path cost to root bridge is 19, Port 2 path cost is 119, 100 (Switch A Port 2) + 19 (Switch B Port 1). For Switch B, Port 1 path cost is 19, Port 2 path cost is 119. Root port = Port 1 of Switch A and Switch B because it has the lowest path cost to the root bridge Switch C.
3. On Segment A, both Port 2 of Switch A and Switch B have the same path cost to root bridge. Since Switch A has lower bridge ID than Switch B, the designated port is selected on Switch A. So Port 2 of Switch A is designated port.
Blocking = Port 2 of Switch B, the non designated port on the segment.
Forwarding = All designated ports and root ports.

All contents copyright 2008 ZyXEL Communications Corporation.

Switching security

MAC Limit

As an added protection against network intrusion attacks, ZyXEL has implemented the MAC limit feature on VES-1616FA-54. Security has been the main focus of our switch design. With the MAC limit feature enabled, dynamic MAC addresses on specified ports are stored in the static MAC address table. At the same time, MAC address learning is disabled on these ports thus denying network access for computers within unknown MAC addresses.
Without the MAC limit function, any computer can access the network through a switch port. The port automatically learns the computer's MAC address and stores it to the MAC address table.
Activate the MAC limit function on a port by entering the port-security [port number] command in the CLI.
The following figure shows an example where the MAC limit feature is enabled on port 6. And port 6 only can dynamic learn 64 MAC addresses.



After you enabled MAC limit on the port 6 using the CLI command, the switch automatically disables MAC address learning on that port. Display the **Port Security** screen to verify this.

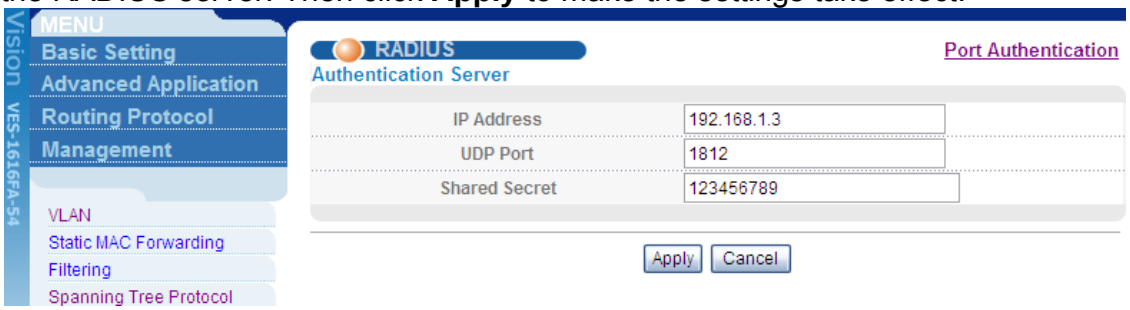
All contents copyright 2008 ZyXEL Communications Corporation.

All contents copyright 2008 ZyXEL Communications Corporation.

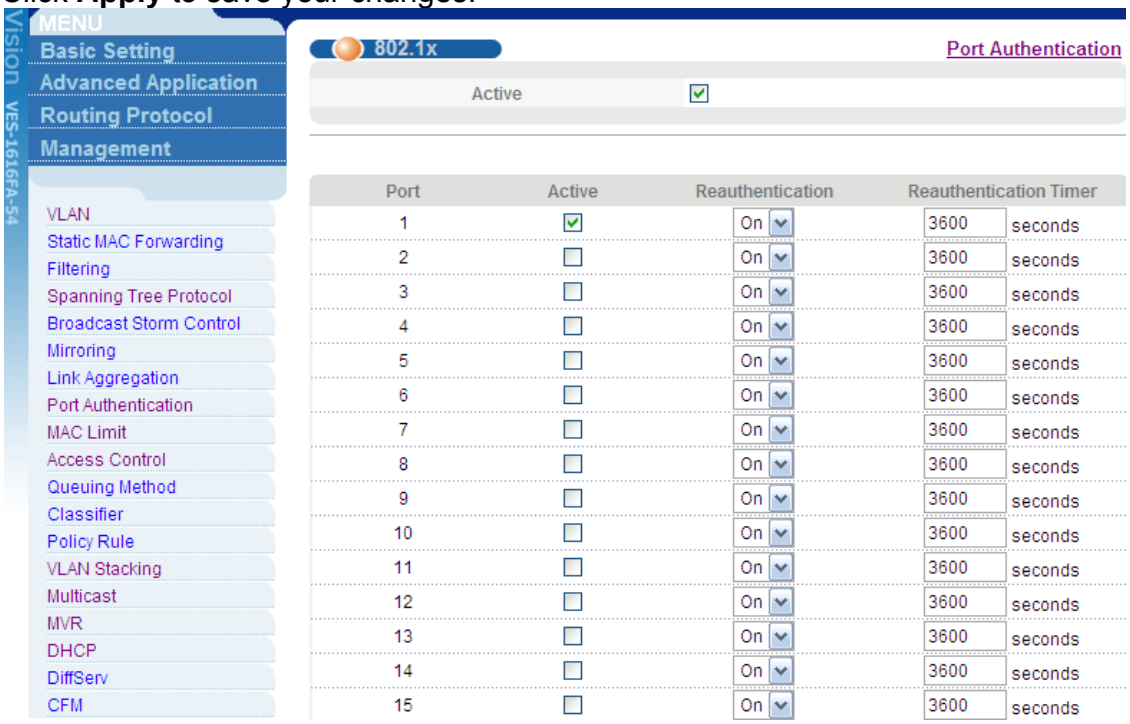
Setting up 802.1x Radius Authentication.

Port Authentication: RADIUS Setup

Click **Advanced Application> Port Authentication** in the navigation panel to display the port Authentication page and click RADIUS link to display RADIUS configuration screen as shown. Set the RADIUS server **IP address**, **UDP port** and **shared Secret**. Make sure the information you have entered is the same as the RADIUS server. Then click **Apply** to make the settings take effect.



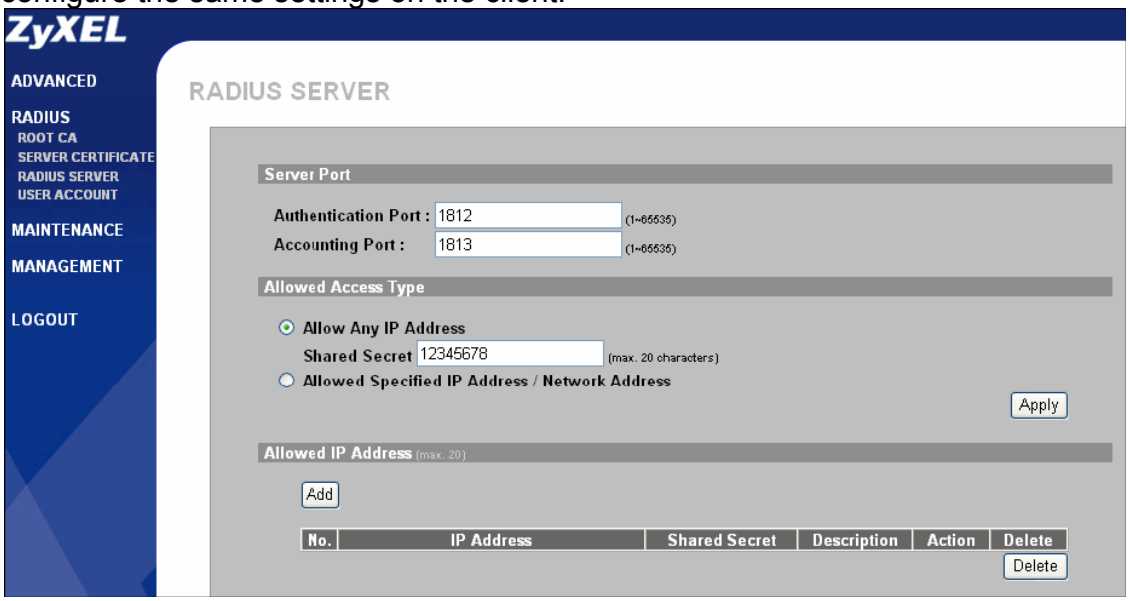
Click the **802.1x** link to display the **802.1x** configuration screen. Select the **Active** check box to enable and then select the **Active** for a port to enable 802.1x authentications on that port. You can leave the other settings to the default values. Click **Apply** to save your changes.



All contents copyright 2008 ZyXEL Communications Corporation.

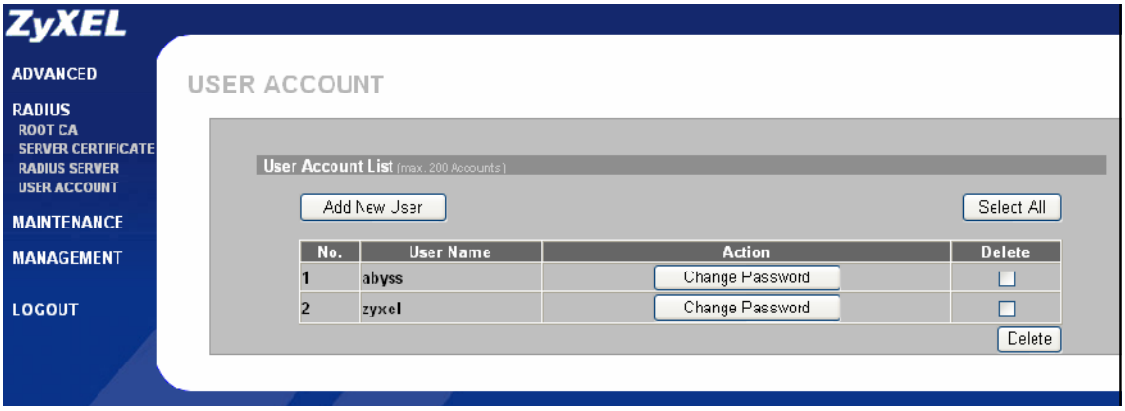
RADIUS Server Setup

Click **RADIUS** > **RADIUS SERVER** in the navigation panel to display the configuration screen as shown. You can use the default values or change the settings in the **Authentication port** and **Shared Secret** fields. Make sure you configure the same settings on the client.



Create User Account

Click **RADIUS** > **USER ACCOUNT** in the navigation panel to display the configuration screen as shown. You can use the existing user accounts or create a new one by clicking the **Add New User** button. Note that the client site MUST use the account in the RADIUS server.



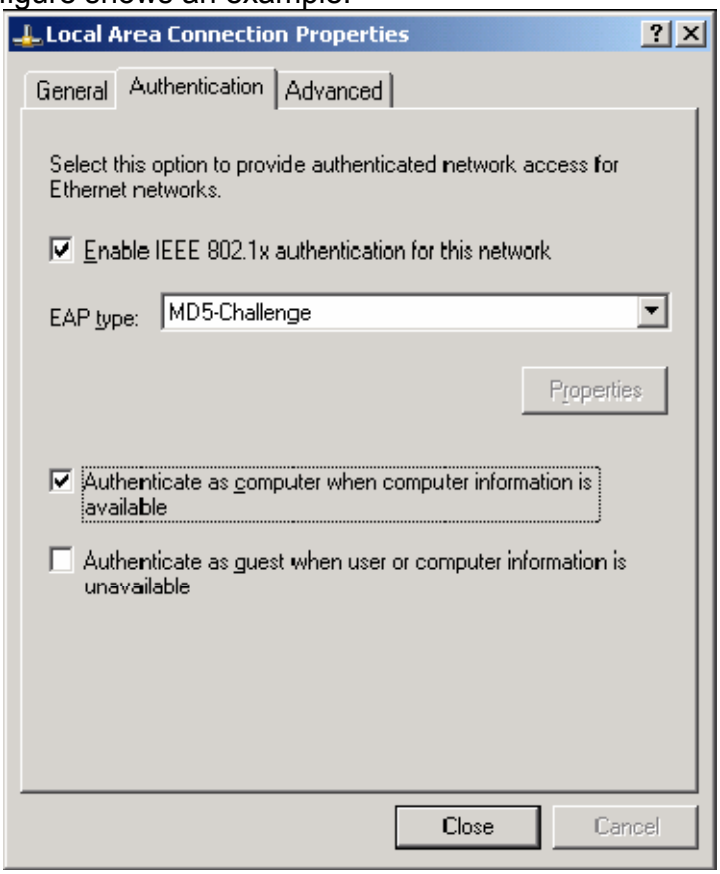
Supplicant Setup (Windows XP)

You can use any supplicant software (such as MeetingHouse Aegis client, Funk Odyssey client and Microsoft 802.1x client). For this example, we will show you how to configure the Microsoft 802.1x client.

All contents copyright 2008 ZyXEL Communications Corporation.

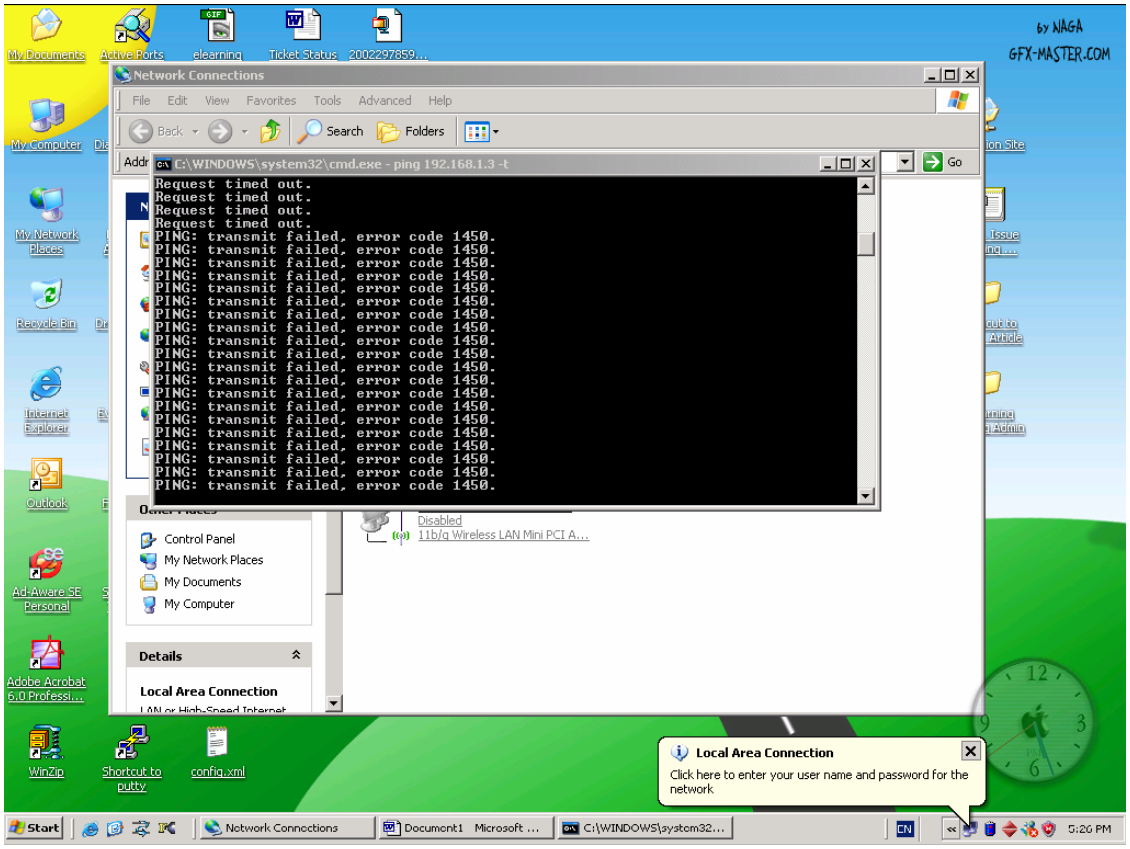
802.1x/MD5-challenge setup

Open the **Local Area connection Properties** screen and click the **Authentication** tab. Select the **Enable IEEE 802.1x authentication for this network** option and select **MD5-challenge** in the **EAP type** field. The following figure shows an example.



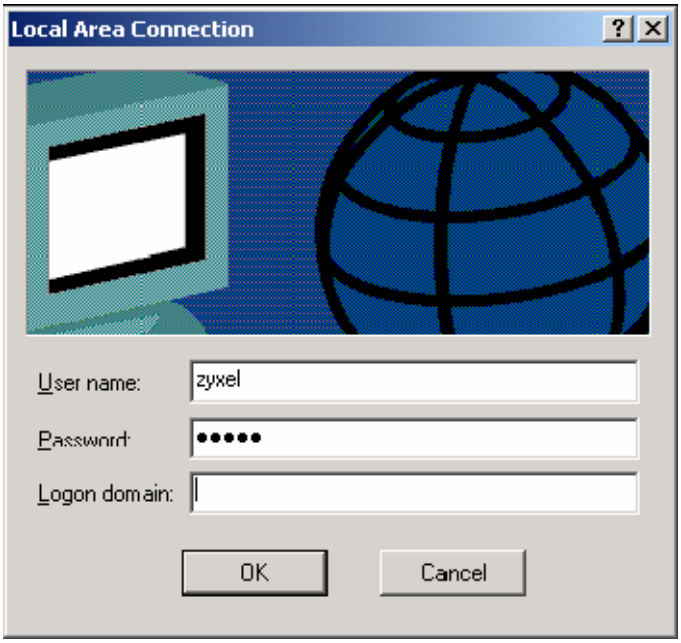
When 802.1x authentication process starts, you are prompted to enter the user name and password. The following figure shows the prompt.

All contents copyright 2008 ZyXEL Communications Corporation.



Click on the message window and a login screen displays as shown. Enter your account user name and password in the fields provided.
After you click **OK** and the authentication server has verified your account, you can log into the system successfully. This indicates that you have configured the client for 802.1x authentication correctly.

All contents copyright 2008 ZyXEL Communications Corporation.



After the configuration, the port is authenticated and the computer connected to this port is allowed to access the network. Otherwise, the computer cannot access the network.

Classifier & Policy rule setup on your Switch

This section shows you how to allow traffic from certain IP addresses and deny others. This can be done easily using classifier and policy rules.

First, you need to create a classifier rule to group traffic into data flows based on information such as the source address, destination address, port number and packet format. In this example, we group traffic based on the packet format and set the VES-1616F-3X to apply its policy rules. The following lists the three classifier rules that we will define in this example:

1. Packet with a source IP address of 192.168.1.20
2. Packets on port 2
3. ARP traffic for testing

Once packet classification settings are done, we create policy rules to specify the actions on the matched packets so they get the deserved treatment in the network. Here, we also define three policy rules.

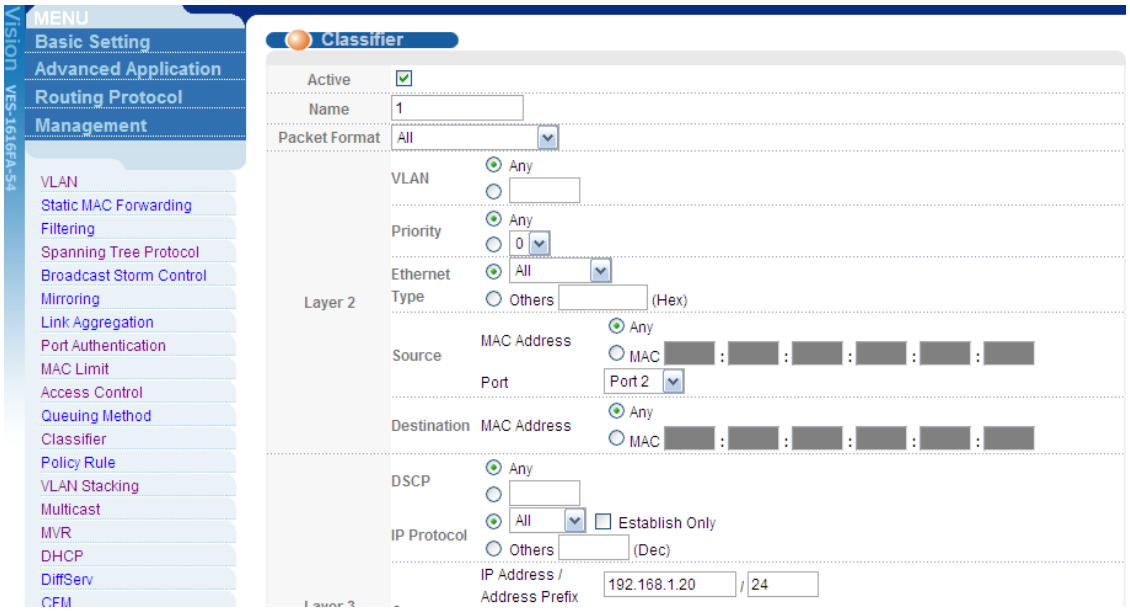
1. Forward traffic from 192.168.1.20 only (on the first classifier)
2. Discard all the traffic from port 2 (on the second classifier)
3. Forward ARP packets (on the third classifier)

All contents copyright 2008 ZyXEL Communications Corporation.

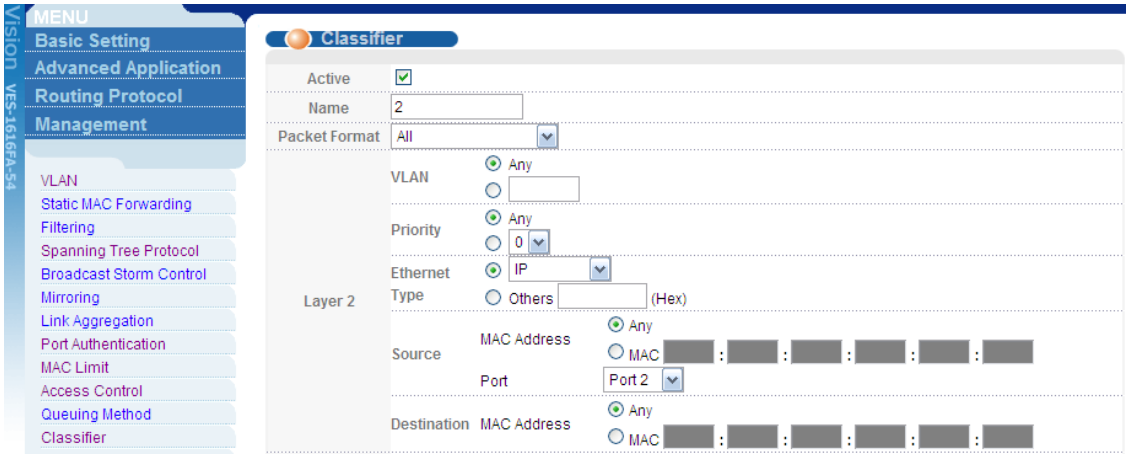
The following figures show the screen settings for each classifier rule.

Classifier Configuration

Classifier 1

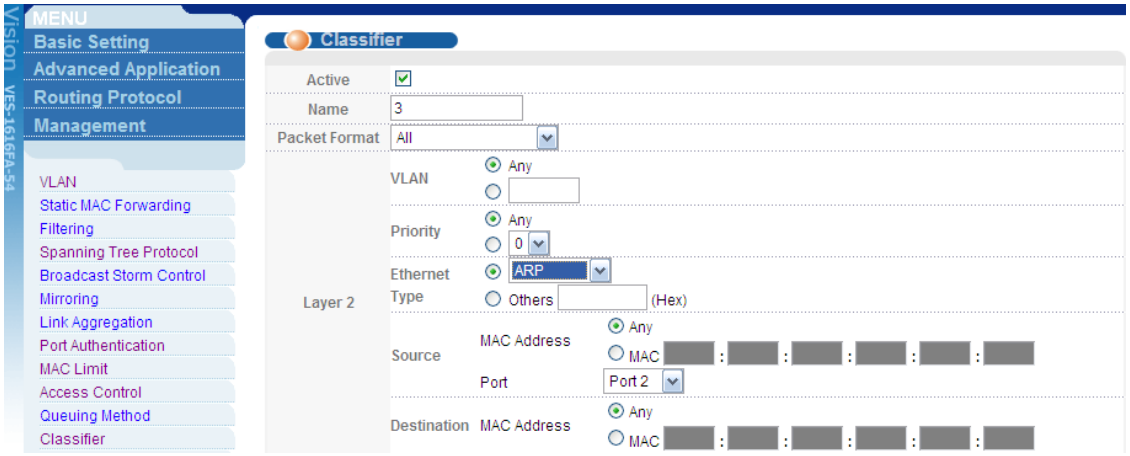


Classifier 2



Classifier 3

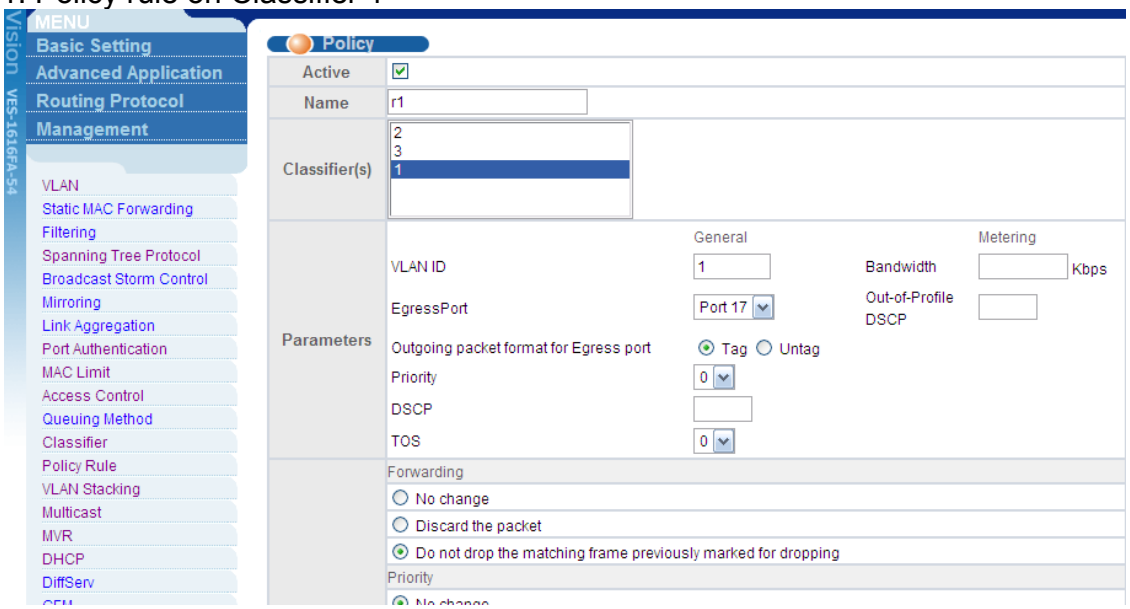
All contents copyright 2008 ZyXEL Communications Corporation.



Policy Rule Configuration

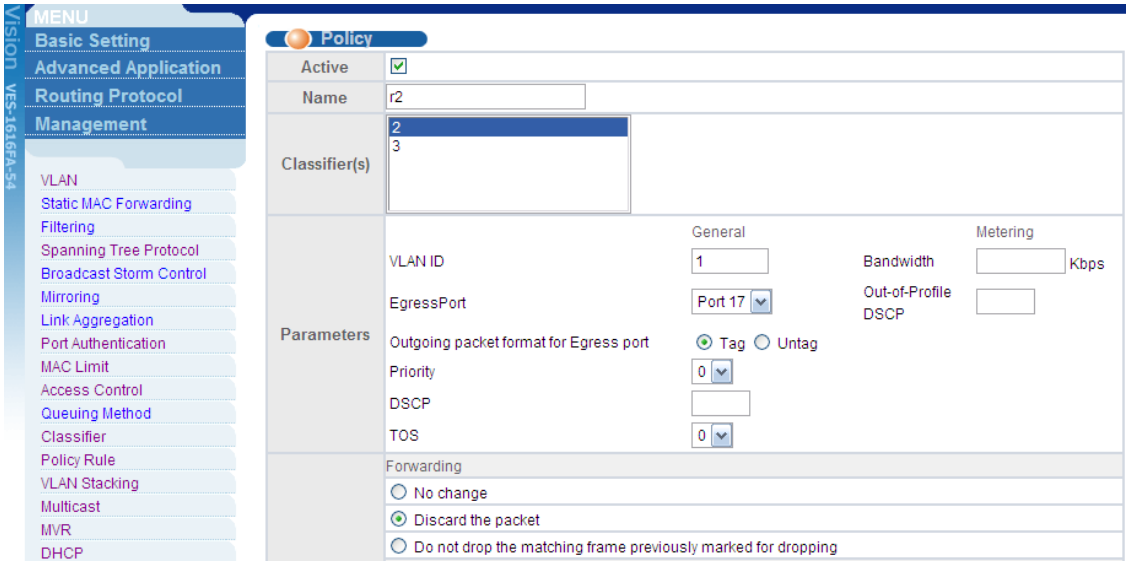
The following figures show the screen settings for each policy rule.

1. Policy rule on Classifier 1

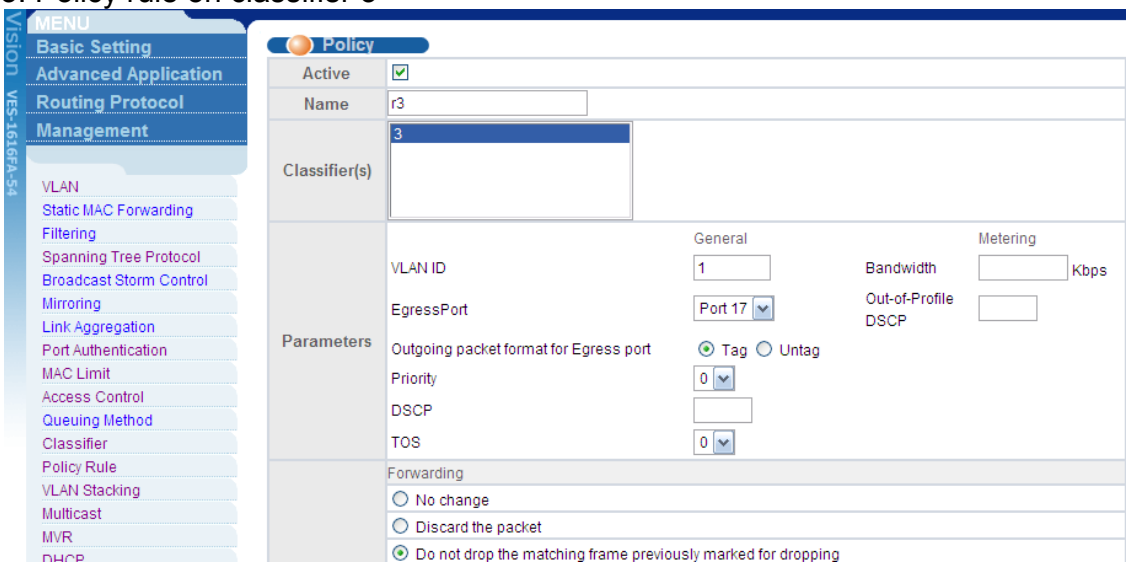


2. Policy rule on classifier 2

All contents copyright 2008 ZyXEL Communications Corporation.



3. Policy rule on classifier 3



Centralized Management

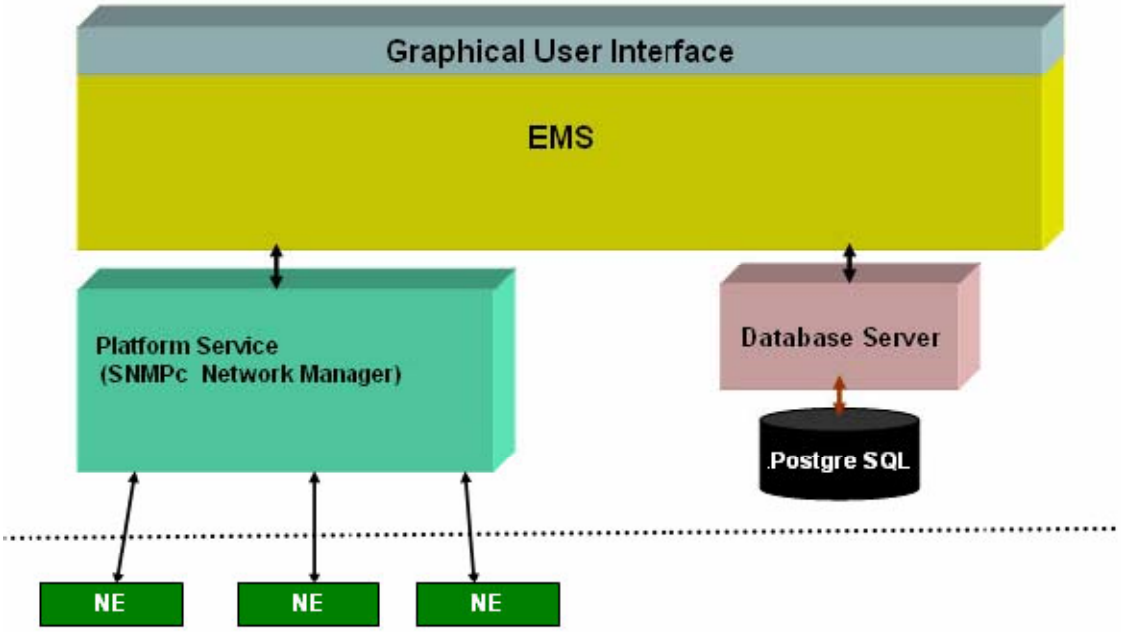
Introduction to SNMPc and NetAtlas

With the number of network device increasing, the demand to detect and respond

All contents copyright 2008 ZyXEL Communications Corporation.

to network failures or events in a short time post a great challenge to network administrators. How to easily manage and monitor network devices across networks has become more and more important in network management. Figure 1 presents the main elements of the system architecture. As an Element Management System (EMS), NetAtlas provides a centralized remote management platform and acts as an SNMPc manager to perform network configuration, system management, event/alarm management, performance management and security for all ZyXEL's Ethernet switches. SNMPc is a network management software produced by Castle Rock that constantly probes the network element (NE) and collects information from these NE for the EMS. Running in the background to provide queries for the EMS is PostgreSQL, an enterprise relational database system

Figure 1 System Architecture



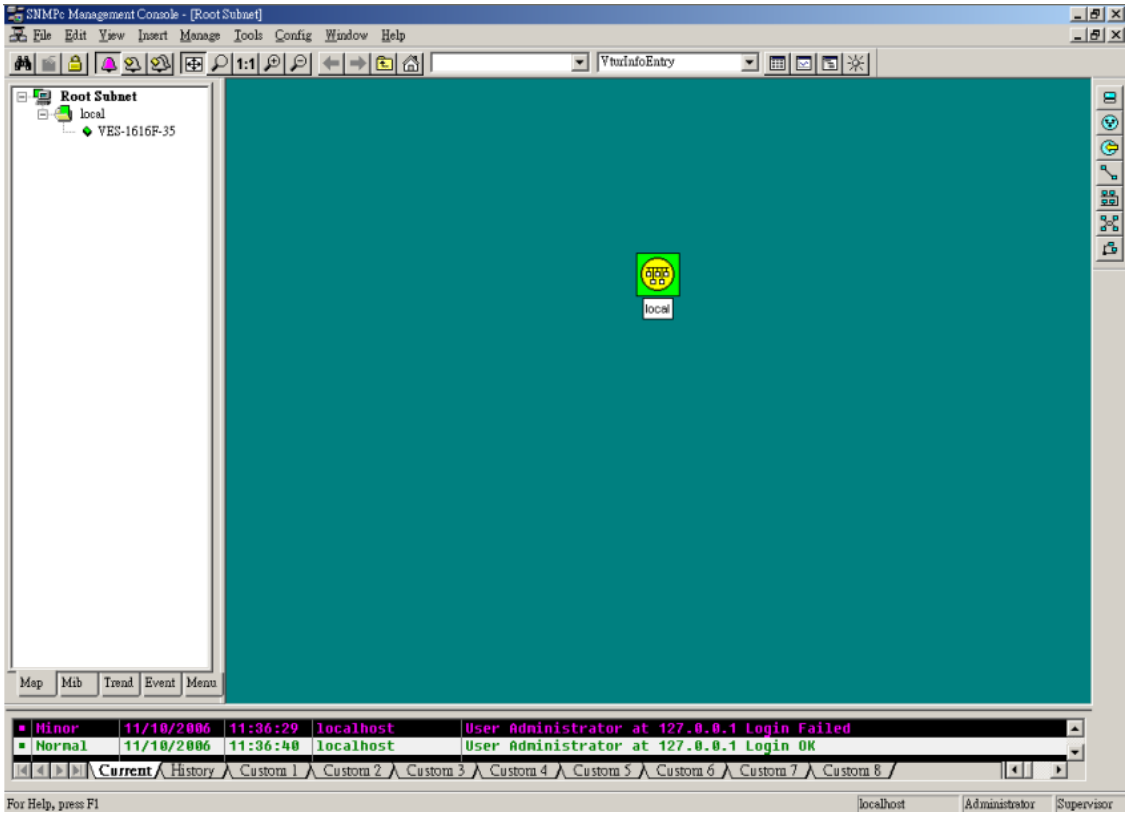
SNMPc Overview

The following figure shows the main screen elements of SNMPc.

- **Main Button Bar**: Button and controls to execute commands quickly
- **Edit Button Bar**: Button to quickly insert map element
- **Event Log Tool**: Button display filtered event log entries
- **View Window Area**: Map View, Mib Tables and Mib Graph windows are displayed here.
- **View Window Area**: Map View, Mib Tables and Mib Graph windows.

Figure 2 Main elements of SNMPc

All contents copyright 2008 ZyXEL Communications Corporation.


SNMPc Management Console - [Root Subnet]
File Edit View Insert Manage Tools Config Window Help
VtuInfoEntry
Root Subnet
local
VES-1616F-35
local
Map Mib Trend Event Menu
Minor 11/10/2006 11:36:29 localhost User Administrator at 127.0.0.1 Login Failed
Normal 11/10/2006 11:36:40 localhost User Administrator at 127.0.0.1 Login OK
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8
For Help, press F1
localhost
Administrator
Supervisor

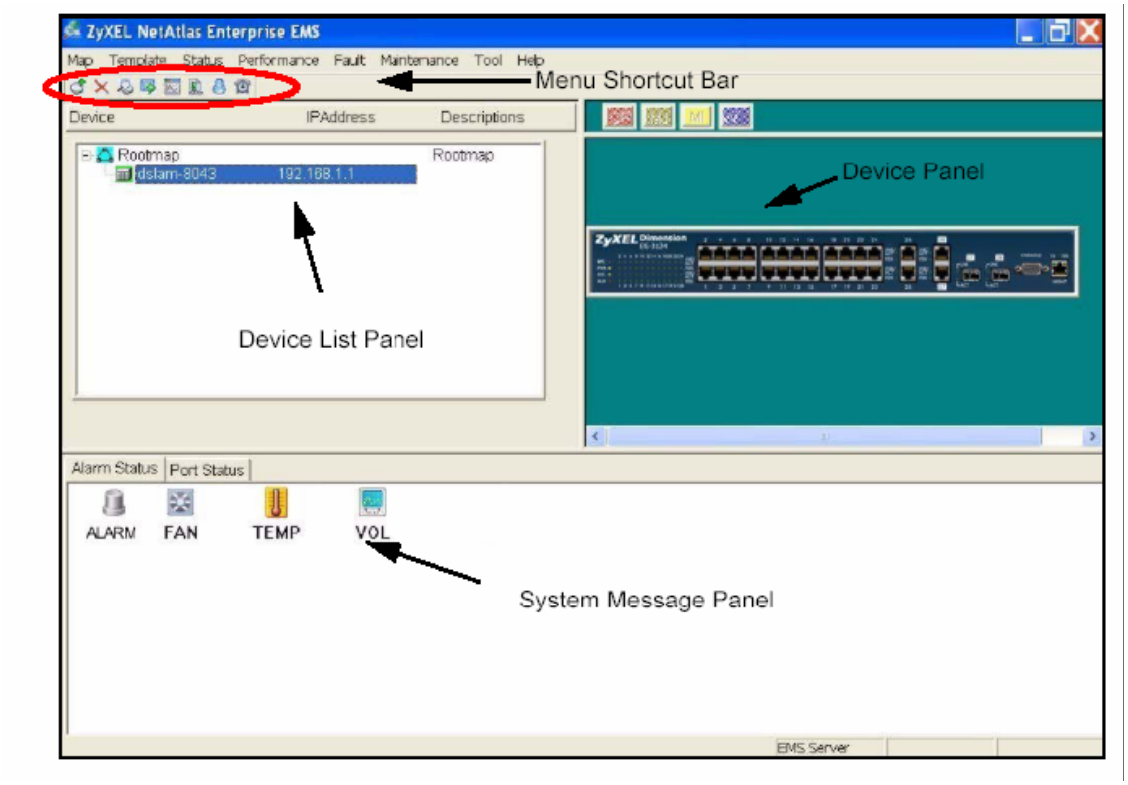
EMS Overview

The following figure illustrates the main elements in the EMS.

- **Menu Shortcut Bar**: The buttons execute common commands
- **Device Panel**: This is a graphical device display.
- **Device List Panel**: View devices in a tree structure. The colors of the device indicate the status of the devices. Green means the device is working properly and Red indicates no response from the device.
- **System message Panel**: View the alarm and port status of the selected switch.

Figure 3 EMS Overview

All contents copyright 2008 ZyXEL Communications Corporation.



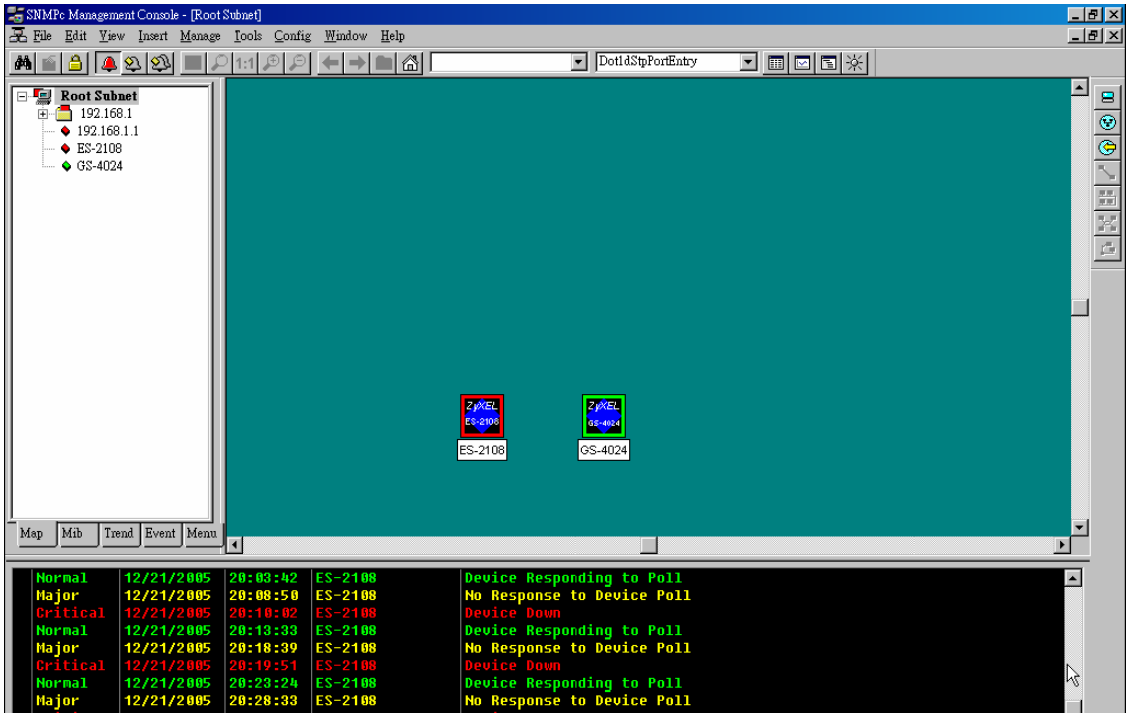
Adding a new device in SNMPc

This section shows you how to add a new device in SNMPc and access the EMS screen.

1. In the edit button bar shown in Figure 4, click the **Insert Device** icon to create a new device node.

Figure 4 Adding a new Device

All contents copyright 2008 ZyXEL Communications Corporation.


SNMPc Management Console - [Root Subnet]
File Edit View Insert Manage Tools Config Window Help
Root Subnet
192.168.1
192.168.1.1
ES-2108
GS-4024
Map Mib Trend Event Menu
ES-2108
GS-4024
Normal 12/21/2005 20:03:42 ES-2108 Device Responding to Poll
Major 12/21/2005 20:08:50 ES-2108 No Response to Device Poll
Critical 12/21/2005 20:10:02 ES-2108 Device Down
Normal 12/21/2005 20:13:33 ES-2108 Device Responding to Poll
Major 12/21/2005 20:18:39 ES-2108 No Response to Device Poll
Critical 12/21/2005 20:19:51 ES-2108 Device Down
Normal 12/21/2005 20:23:24 ES-2108 Device Responding to Poll
Major 12/21/2005 20:28:33 ES-2108 No Response to Device Poll

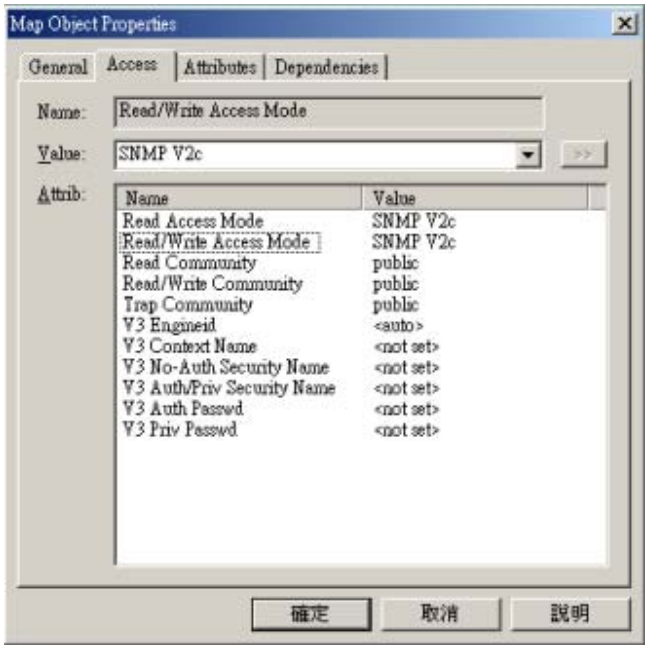
2. A **Map Object Properties** screen displays. Enter a descriptive name in the **Label** field. Then enter the IP address of the device in the **Address** field. For this example, we enter “192.168.0.1” as the IP address of the switch.

Figure 5 Map Object Properties

3. Click the **Access** tab to configure SNMP settings. Change the value for **Read Access Mode** to **SNMP V2c**.

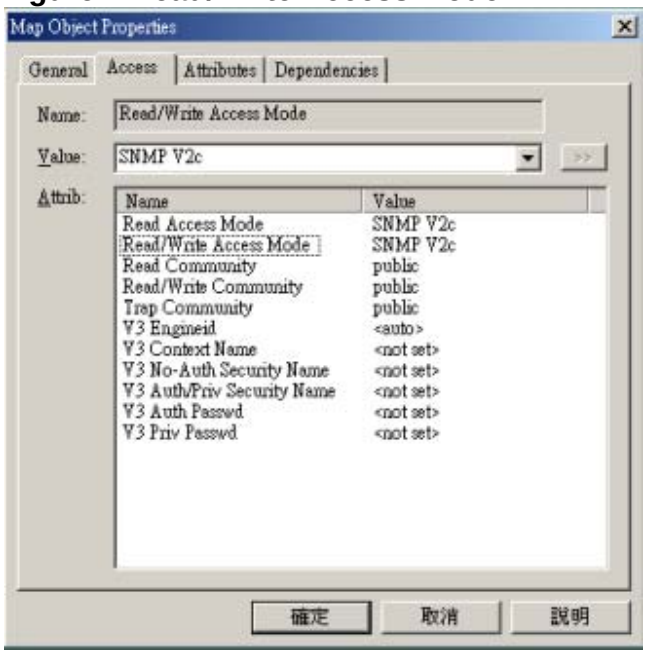
Figure 6 Read Access mode

All contents copyright 2008 ZyXEL Communications Corporation.



4. Change the value for **Read/Write Access Mode** to **SNMP V2c**. Screen settings should be similar to the one shown.

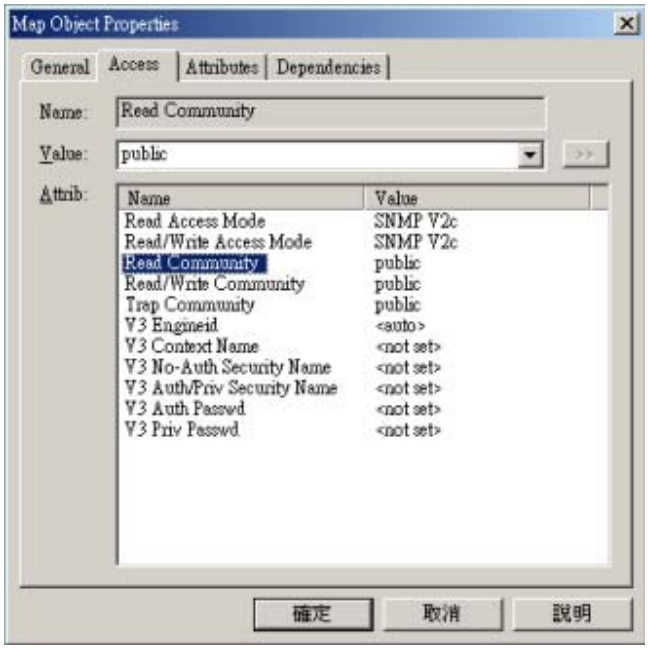
Figure 7 Read/Write Access Mode



5. Change the value for **Read Community** to **public**.

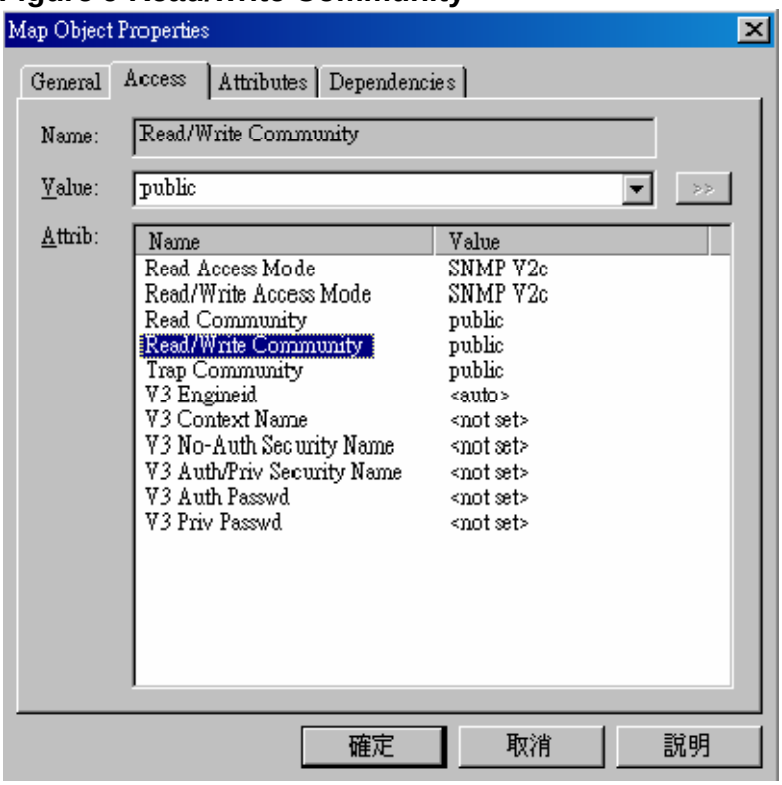
Figure 8 Read Community

All contents copyright 2008 ZyXEL Communications Corporation.



6. Change the value for **Read/Write Community** to **public**. Click **OK** to save the settings and close this screen.

Figure 9 Read/write Community



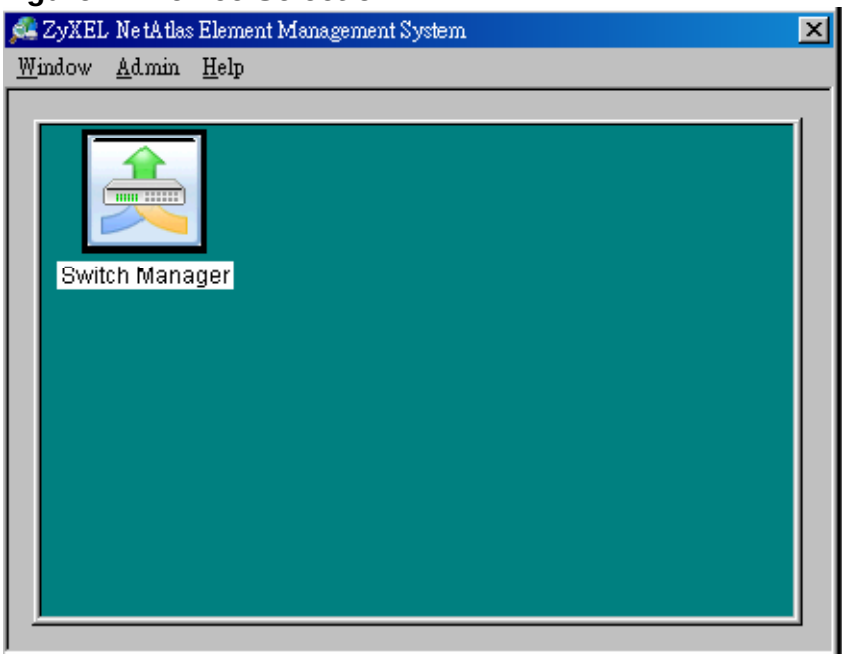
7. In the Selection tool menu, click the name of the switch you have just created to manage the device.

All contents copyright 2008 ZyXEL Communications Corporation.

Figure 10 Device Selection

8. A screen displays as shown. Click **Switch Manager** to display the main EMS screen as shown in Figure 11

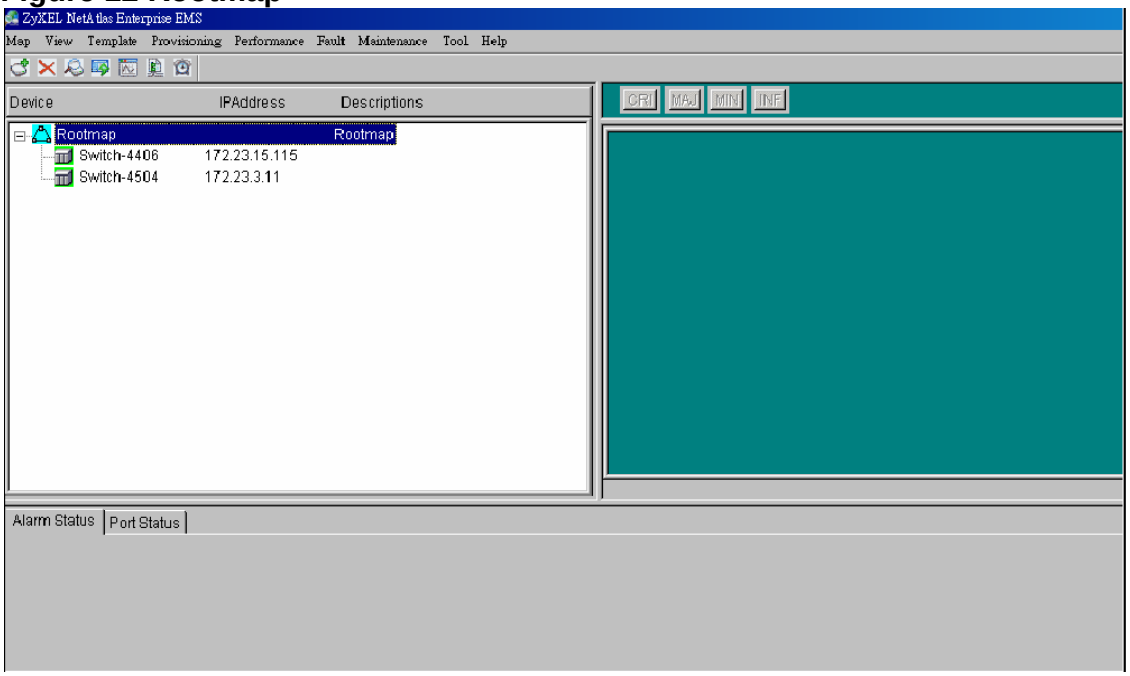
Figure 11 Device Selection



9. The device list panel on the left displays a logical hierarchy of the devices. You can also see the devices added under the Rootmap in this list. Figure 12 shows an example.

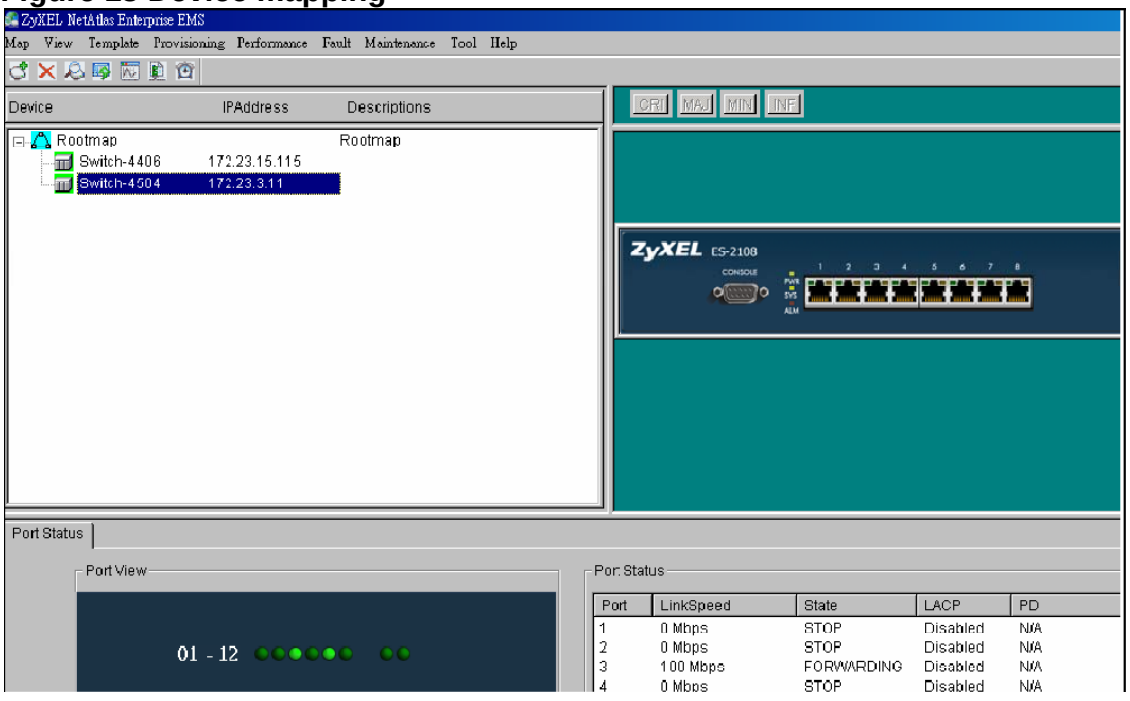
All contents copyright 2008 ZyXEL Communications Corporation.

Figure 12 Rootmap



10. Click on a switch icon to display the device panel and status screen as shown in Figure 13.

Figure 13 Device mapping



All contents copyright 2008 ZyXEL Communications Corporation.

FAQ

What are the default IP parameter settings?

IP address: 192.168.1.1
Subnet: 255.255.255.0

What is the default login Name and Password to log into the Web Configurator?

ID: admin
Password: 1234

How to access my SWITCH through the console port?

Connect the male 9-pin end of the console cable to the console port of the switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer. Launch a terminal emulation software configured to the follow settings:
Terminal emulation: VT100
Baud rate: 115200 bps
Data bits: 8
Parity: none
Stop bit: 1
Flow control: none

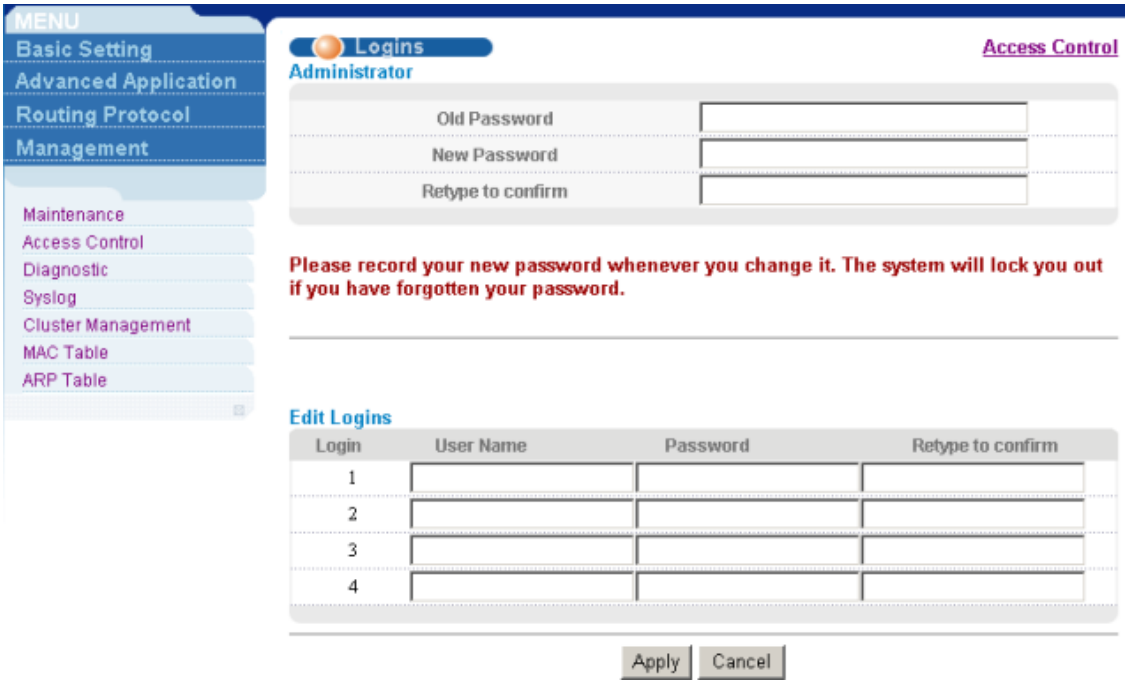
What is default login password for console, telnet, and FTP login?

Password: 1234

How to change the password?

You can only change the administrator login password in the web configurator.. After you log in for the first time, it is recommended you change the default administrator password.
In the Web Configurator: Click **Management > Access Control > Logins** to display the configuration screen as shown. Then change the password by settings the password fields.

All contents copyright 2008 ZyXEL Communications Corporation.



How to access the Command Line Interface (CLI)?

There are two ways to access the Command Line Interface: through the console port or Telnet.
If you want to access through the console port, Refer to the “How to access the Switch through the console port?” section for more information.

If I have forgotten the password, how to reset the password to the default setting?

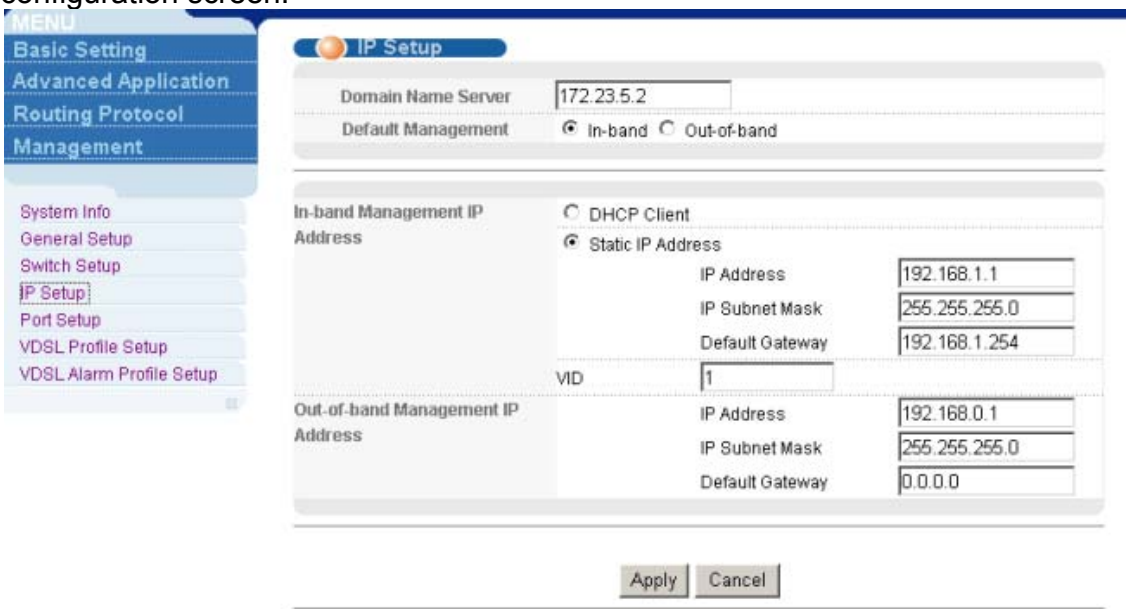
If you have changed and forgotten the password, you will need to reload the factory default configuration. Note that all your previous configuration will be lost.
1. Connect the console cable to your computer and launch a terminal emulation software.
2. Restart the switch, and press any key to enter the debug mode at the “Press any key to enter Debug Mode within 3 seconds” prompt.
3. Enter “atlc”.
4. When the “starting XMODEM upload” message displays, start XMODEM upload of the default configuration (rom) file to the switch.
5. After the file upload process is complete, enter “atgo” to exit from the debug mode.
6. The system will automatically restart. Wait until the system has restarted before you log in again. The default IP address is 192.168.1.1 and the default password is 1234.

How to configure the IP address?

All contents copyright 2008 ZyXEL Communications Corporation.

Using the Web Configurator

Click **Basic Setting > IP Setup** in the navigation panel to display the configuration screen.

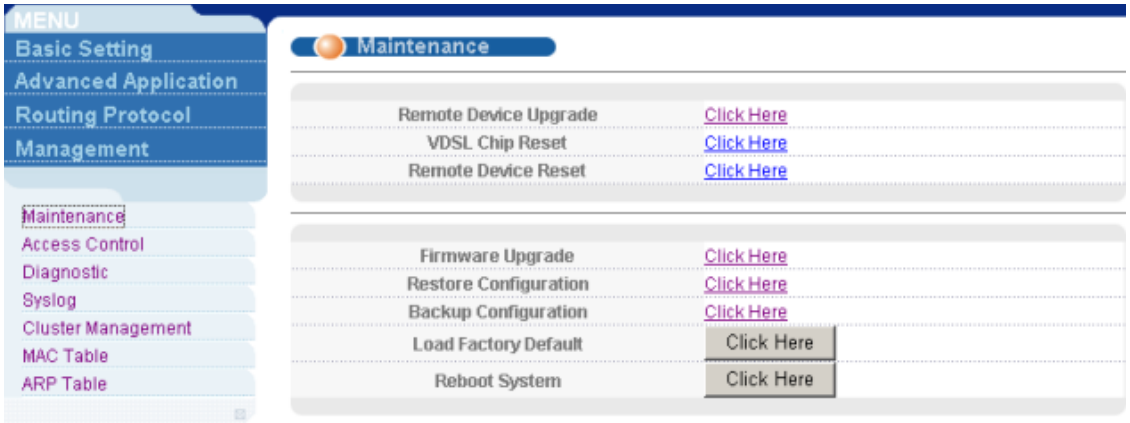


Is Online Help available on the Web Configurator?

Yes. You can click on the Help link in any web configurator screen to display the help content for that screen.

How to restart device from the Web Configurator?

1. Click **Management > Maintenance** in the navigation panel to display the screen as shown.



2. Click **Click Here** button next to **Reboot System** will restart the switch.

How to check the current running firmware version?

All contents copyright 2008 ZyXEL Communications Corporation.

Access the console and enter the “show system-information” command. This will display the firmware version the switch is currently using.

Is the mini GBIC transceiver hot-swappable?

Yes, it is hot-swappable. You can change transceivers while the switch is operating.

What is "Dual-Personality interface" on a VDSL Switch?

Dual-Personality GbE interface means that one 1000Base-T Copper port and one SFP port shares the same physical interface. Only one of them can be used at a time. Dual-Personality interface is also known as a "Combo Port".

Can I enable IGMP snooping on the Switch which is acting as an IGMP Router?

No. You do not need to enable IGMP Snooping on an IGMP Router. IGMP Snooping should be enabled on the access layer device, which is normally a L2 switch.

Can I enable MVR and IGMP snooping at the same time?

Yes.

All contents copyright 2008 ZyXEL Communications Corporation.